UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.

CAMPUS ARAGÓN

ALGUNOS MÉTODOS PARA TENER UNA ÓPTIMA SEGURIDAD EN EL ENVÍO DE DATOS A TRAVÉS DE LA RED INTERNET.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A N:

JUVENAL RODRÍGUEZ MORENO

MIGUEL ÁNGEL TOLEDO HUERTA

DIRECTOR: ING. ELEAZAR MARGARITO PINEDA DÍAZ

San Juan de Aragón. Edo. De México. Julio de 2003

A

A mis padres:

A ustedes, que a pesar de que la vida les ha puesto pruebas difíciles no les impidió hacer de mi un hombre de bien. Por darme la libertad de escoger lo que para mi es lo mejor, por sus consejos, y por que si este trabajo les arranco una sonrisa o una lagrima entonces todos los sacrificios valieron la pena.

A mi hermana Magda:

Por que desde niño me enseñaste que la familia es primero, que las decisiones que uno tome en la vida hay que defenderlas a pesar de lo que digan los demás, por que siempre me diste tu apoyo a pesar de las adversidades, por ser un ejemplo para mi y por que sin ti simplemente este trabajo no lo hubiera podido realizar.

A mis hermanos:

Por que de cada uno de ustedes tengo algo que me ayuda a superarme y ser mejor en la vida.

A mis amigos:

Miguel Ángel "TOLEDO", Edgar, Alejandro "GÜEREJA", Gabriel "PELUCHES", Arturo "MUDO", Julio "TITA", Pablo "TAKESHI", Juan "BALBOA" y Ricardo por compartir tantas cosas conmigo, por su confianza, amistad y hacer de la universidad una experiencia única e irrepetible.

A Paola:

Por darme la oportunidad de conocerte y ser parte de ti, por todas esas cosas buenas y malas que compartes conmigo, por tu amor que es indispensable para mi y por que este trabajo significa que los objetivos a largo plazo se hacen de corto plazo.

A Wendy:

Por todos estos años de amistad, por que siempre tienes las palabras correctas a la hora de darme un consejo que me ayude a ser mejor cada día y por que siempre has querido lo mejor para mi.

Al Profe Asdrúbal y Jaime:

Gracias por escucharme cuando tuve algo que decir y aconsejarme en un momento difícil de mi vida. A usted profe por brindarme su amistad durante estos años. A ti Jaime por enseñarme a comprometerme con mi mismo y tratar de ser siempre el mejor tanto en el deporte como en la vida misma.

Este pequeño logro en mi vida va dedicado muy en especial a cinco personas:

A mi mamá por todo en lo que me has ayudado y me has dado, por estar siempre conmigo, cuidarme, apoyarme en todo, y por todo ese cariño que me has dado.

A mi padrino Oscar (Parri) †† por su gran calidad de ser humano y por ser mi fuente de inspiración para superarme cada día más y por que fuiste y siempre serás mi héroe.

A Margarita por todo lo que me diste y por ser como mi segunda mamá y mi modelo a seguir para superarme cada vez más y ser alguien cada vez mejor en la vida.

A Magali por todos tus consejos y por ser la mejor de todos y en todo. Te quiero mucho.

A mi hermano Arturo por enseñarme a querer superarme, por estar conmigo y por ser como eres.

A mis primos (as):
Alejandra, Roxana, Rosi, Oscar, Pol, Enrique, Álvaro y mi tía Oli por estar conmigo, por todo su apoyo, cariño y ayuda que me han dado en todo este tiempo.

D

A mis hermanos:
Zaid y Carlos por esa gran amistad incondicional que me han brindado todos estos años, por estar siempre conmigo en todo momento, en las buenas y en las malas, (en las borracheras y en las crudas también), por confiar y creer en mi, y por apoyarme en todo lo que he hecho y quiero hacer.

A mis amigos (as):
Brenda, Karla, Erika Paola, Erika Patricia, Anel, Adriana, Ariana, Jorge, Pepe (weeked), Julio Cesar H.P., Pablo (takeshi), Alejandro (mhijo), Juvenal, Edgar (cachetes), Gabriel (pelucas), Ricardo, Arturo (mudo), gracias a todos ustedes por lo más importante, por brindarme su gran amistad y por estar conmigo apoyándome en todo, por todos esos buenos ratos que hemos pasado, por hacerme reír y por ser mis amigos.

A la Universidad Nacional Autónoma De México, a la ENEP Aragón y a los profesores e Ingenieros que imparten clases, gracias por todos los conocimientos adquiridos y por enseñarme a tratar de ser una mejor persona y a poder enfrentar todos los obstáculos que se me presenten.

E

ÍNDICE

INTRODUCCIÓN

A través de la historia hubo necesidad de asegurar la información. Desde las épocas del emperador romano Julio Cesar se utilizó el primer sistema de seguridad en el envío de sus mensajes del que existe conocimiento. El sistema, bastante fácil de adivinar, consistía en intercambiar cada letra del alfabeto por aquella que distaba un número fijo de posiciones a izquierda o derecha dentro del mismo; por ejemplo, un desplazamiento de dos posiciones a la derecha en la palabra ataque producía el siguiente juego de letras: cvcswg; es decir, cada letra de la palabra ataque se sustituía por la letra que se encuentra a dos lugares a la derecha del alfabeto.

Desde los inicios de la era de la computación, los sistemas de seguridad para acceso a la información se han basado en el rudimentario y efectivo método de proporcionar un nombre de usuario y una clave secreta. Estos sistemas tan sencillos han sido bastante eficaces mientras que toda la información sensible residía en los ordenadores centrales y los terminales de acceso se situaban localmente cerca del ordenador central o como máximo accedían por líneas dedicadas.

El crecimiento de Internet como un conjunto de redes y subredes que componen el sistema utilizado para localizar y tener acceso a las fuentes de información de Internet ha aumentado los riesgos de la seguridad y se ha sensibilizado tanto a las organizaciones privadas y gubernamentales hacia la búsqueda de medidas de seguridad electrónicas adicionales. En realidad, son un conjunto de tendencias tecnológicas las que han convergido no sólo para mostrar la necesidad de dotar de mecanismos de seguridad a las comunicaciones electrónicas, sino que están cambiando la forma de los sistemas de información actuales. Algunas de éstas tendencias son:

- Uso creciente de infraestructuras públicas de bajo costo para comunicaciones de datos.
- Cambio de un sistema centralizado a un sistema distribuido.
- Proliferación de computadores personales, portátiles, y usuarios que acceden remotamente.
- Aumento en el número y tamaño de las redes de área local y de las redes de área extensa.
- Aumento del interés de realizar operaciones de comercio electrónico por Internet.
- Mayor aceptación por parte de los usuarios de realizar transacciones electrónicamente.

Desde el punto de vista de la seguridad en el envío de datos, el impacto más importante de dichas tendencias ha sido:

- Los usuarios ya no se encuentran conectados localmente a los sistemas de información del Internet. Ahora se pueden conectar a la red Internet desde su casa, en la habitación de un hotel, en el coche, etcétera. Sin embargo, un usuario no sabe si está conectado en Internet a través de un ordenador al final de la calle o en el extremo opuesto del mundo.
- El intercambio de información abre sus fronteras más allá de la empresa, sobre todo desde la aparición del correo electrónico.
- Existe un gran número de sistemas de redes de comunicaciones, como lo puede ser: líneas de teléfono, comunicaciones inalámbricas o comunicaciones vía satélite por donde fluye la información.

Ningún tipo de compañía, ya sea grande o pequeña, puede darse el lujo de correr riesgos de seguridad en su red. Sin embargo, los costos financieros de una seguridad inadecuada pueden ir mucho más allá de los costos de invertir en soluciones de protección. Los expertos estiman que solamente las empresas en los Estados Unidos gastaron cerca de $12.3 mil millones de dólares para reparar el daño de virus de computadoras y de información o mensajes interceptados por intrusos del Internet en el 2002, y los ataques futuros de virus podrían causar aún más estragos en el 2003. Nadie es inmune a la amplia gama de actos maliciosos posibles. Por lo tanto, las compañías deben enfrentar la realidad de que sus redes, datos y usuarios podrían verse comprometidos a través de una amplia gama de ataques maliciosos. Por lo dicho anteriormente, es prudente controlar el acceso de los usuarios y filtrar el tráfico de la red, sin importar si éste se origina desde el interior del perímetro electrónico corporativo o en alguna parte del Internet.

El objetivo principal de este proyecto de tesis es, como su título lo indica, el de dar a conocer algunos métodos de seguridad en el envío de cualquier tipo de datos a través de la red Internet, como lo son los métodos de: seguridad con cifrado y firmas, seguridad con el protocolo de Internet, seguridad con encriptamiento, y seguridad con autenticación; para así poder asegurar que dichos datos enviados por cualquier emisor lleguen lo más seguro posible a su receptor indicado, sin ser leídos o interceptados, y sin sufrir ningún tipo de alteración o modificación; así también, proporcionar información acerca de los tipos de amenazas y ataques existentes en la red Internet. Otro objetivo que se plantea es el de reducir al mínimo los riesgos de que el intruso de la red Internet obtenga información que no le corresponda, utilizando algunos de los métodos explicados en este proyecto de tesis.

Dicho proyecto de seguridad en el envío de datos a través de la red Internet ha sido pensado en las pérdidas económicas millonarias que se suele tener en alguna empresa o negocio debido a que la información confidencial puede llegar a ser captada o interceptada por los llamados intrusos de la red Internet. Hay que aclarar, que en este

proyecto de tesis se mencionan solo los aspectos y/o las características que a nuestro parecer son los más importantes de los métodos mencionados anteriormente.

La información que se presenta en este proyecto de tesis, puede ser utilizada por cualquier tipo de empresa o compañía, o incluso para uso personal de los usuarios de la red Internet que se sientan agredidos a una posible intercepción de sus mensajes, datos o información enviada por la red Internet.

En el capítulo I se explica lo que es la seguridad en redes, algunas de las amenazas y ataques existentes en la red Internet, como poder protegerse o evitar dichos ataques y amenazas; así también se mencionan términos que son necesarios para comprender la información en los capítulos posteriores.

En el capítulo II se menciona como tener seguridad en el envío de datos a través de la red Internet con algunos métodos de cifrado y firmas digitales, dando una breve explicación de su funcionamiento así como los elementos en que se apoya el cifrado y las firmas.

El capítulo III se refiere al método de seguridad con el protocolo de Internet, mencionando brevemente elementos importantes como lo son sus modos de transmisión, algunos de sus aspectos importantes como lo es el ámbito en el que trabaja y algunas de sus aplicaciones, así también el cómo está constituida su cabecera de autentificación.

En el capítulo IV se menciona la seguridad en el envío de datos a través de la red Internet con el método de encriptamiento, mencionando, sin entrar a detalle, algunos de sus algoritmos, algunos métodos de encriptamiento en correo electrónico más conocidos actualmente, así como características importantes sobre la seguridad con encriptamiento.

En el capítulo V se mencionan brevemente las herramientas que utiliza el método de autenticación para dar seguridad en el envío de datos a través de la red Internet, dichas herramientas son algunos protocolos, un servicio de marcación para usuarios remotos, dos sistemas, uno de ellos es el sistema de control de acceso y otro sistema de distribución de claves, certificados y tarjetas inteligentes.

CAPÍTULO I
GENERALIDADES

El objetivo principal de la seguridad en el envío de datos a través de la red Internet es el de proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Esto incluye los equipos, los medios de almacenamiento, el software, los listados de impresora y la información. La seguridad en redes abarca un amplio rango de estrategias y soluciones, tales como:

- Control de acceso: control de la entrada al sistema.
- Control de acceso discrecional: control de acceso a los recursos tales como archivos y programas, una vez que se encuentra dentro del sistema.
- Virus: diferentes clases de virus y otros programas destructivos, además de prevenir y controlar sus efectos.
- Cifrado: el cifrado y descifrado de la información, de forma que sólo las personas autorizadas puedan accesar a dicha información.
- Planificación y administración del sistema: planificación, organización y administración de los servicios relacionados con las computadoras, así como políticas y procedimientos para garantizar la seguridad en la red.
- Seguridad física: asegurar los equipos y los servicios informáticos.
- Biométricas: utilización de características para identificar a los usuarios.
- Seguridad de la red y de las comunicaciones: problemas de seguridad en las comunicaciones a través de las redes y los sistemas de comunicaciones.

La seguridad es un elemento importante de cualquier servicio y/o sistema informático, pero es considerado como algo que puede hacerse más tarde. Sin embargo, una única brecha en la seguridad puede crear graves daños, o incluso la ruina de alguna empresa. El costo de la recuperación y la pérdida de productividad puede ser sustancial. El papel de la seguridad informática será tan importante que no

podrá ser ignorado, especialmente por el aumento de la exposición al riesgo, debido a las redes y a la integración con las comunicaciones.

I.1 SEGURIDAD EN REDES

Mientras continúa aumentando el tamaño de las redes de computadoras y su integración con otras redes, los retos para mantener la seguridad de los datos aumentan significativamente. Aunque la interconexión y la conectividad han hecho más fácil comunicar y compartir datos, también se expone a muchos ataques contra la seguridad que pueden herir o dañar los sistemas informáticos y los datos. Las redes están conectadas al mundo exterior a través del Internet y mecanismos de integración de la telefonía y las computadoras.

Esto hace que las personas del mundo exterior tengan más posibilidades de obtener acceso a los servicios informáticos o a datos, incluso aunque no tengan ninguna relación con la empresa con cuyas computadoras intentan establecer contacto. Los piratas informáticos, los intrusos de la red Internet, los antiguos empleados, etc, tienen el potencial de conectarse a las facilidades de datos.

La seguridad en las redes de Internet está relacionada con la seguridad de los sistemas, programas y datos cuando éstos existen en una red establecida. Cuando las máquinas se conectan por una red de área local, una red de área extensa, o módem, hay asociados una serie de riesgos de seguridad.

Los requisitos en la seguridad de la información dentro de un organismo han sufrido principalmente dos cambios en las últimas décadas. Antes de que se extendiera la utilización de los equipos de procesamiento de datos, la seguridad de la información, que era de valor para una institución, se conseguía por medios físicos y administrativos. Un medio físico es el uso de las cajas fuertes con combinación de apertura para

almacenar documentos confidenciales; un medio administrativo es el uso de procedimientos de investigación de personal durante la fase de contratación.

Un aspecto importante, que ha afectado la seguridad en el envío de información, es la utilización de redes y las facilidades de comunicación para transportar datos entre terminales de usuario y computadores, y de computador a computador. Las medidas de seguridad en redes son necesarias para proteger los datos durante su transmisión y garantizar que los datos transmitidos sean auténticos.

La seguridad es importante en los sistemas financieros, sin importar si se basan en transacciones físicas o electrónicas. En el mundo real dependemos mucho de la seguridad física, pero en el del comercio electrónico tenemos que depender aún más de los medios electrónicos para proteger los datos, comunicaciones y transacciones. Cuando se trabaja en el mundo de las computadoras en red, son varios los tipos de amenazas para la seguridad de los sistemas. La tabla I.1 menciona algunas de estas amenazas y soluciones de seguridad. Algunas soluciones proporcionan un buen grado de seguridad, incluso para aquellos no involucrados en el comercio electrónico, por ejemplo, la gente que necesita enviar información confidencial de negocios vía correo electrónico. Hay que usar los medios electrónicos para proteger los datos, comunicaciones y transacciones.

Amenaza.	Solución para la seguridad.	Función.	Tecnología.
Datos interceptados, leídos o modificados ilícitamente.	Encriptamiento.	Los datos se codifican para evitar su alteración.	Encriptamiento simétrico; encriptamiento asimétrico.
Los usuarios asumen otra identidad para cometer un fraude.	Autentificación.	Verifica la identidad del receptor y emisor.	Firmas digitales.

Tabla I.1 Algunas amenazas a la seguridad y soluciones

Desde hace mucho tiempo se sabe que Internet depende de estándares abiertos. Este apoyo a los estándares abiertos, junto con el intercambio abierto de información en Internet, puede hacer que uno piense que seguridad e Internet son términos mutuamente excluyentes.

Aunque en el pasado Internet instrumentó menos seguridad que las redes privadas de valor agregado, o las redes corporativas, los esfuerzos por proporcionar una variedad de mecanismos de seguridad al tráfico en Internet han progresado a toda velocidad. Más y más medidas de seguridad se están instrumentando en Internet. Parece como si Internet hubiera ganado un exceso de riquezas en cuanto a la seguridad, con una variedad de estándares que cubren muchos niveles de redes, desde

la seguridad al nivel de paquete, hasta la seguridad al nivel de aplicación. Aunque todavía se considere a Internet como un medio inseguro, debido a su naturaleza descentralizada, es importante señalar que los datos involucrados en las transacciones que usen estos protocolos pueden estar seguros.

I.2 ALGUNOS TIPOS DE AMENAZAS EN LA RED INTERNET

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso ilegítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red se pueden caracterizar modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.

Las amenazas contra la seguridad de los sistemas distribuidos son desafiantes. Los diferentes tipos de sistemas de red en uso hacen difícil implementar medidas de seguridad consistentes en ellos dentro de una empresa u organización, y una seguridad centralizada de la red es esencialmente comprometida. Por ejemplo, si alguien o cualquier proceso necesita enviar datos a través de la red Internet para ejecutar medidas de seguridad, solamente la transferencia a través de la red hace sospechoso al sistema completo.

Estos son algunos tipos de amenazas comunes a la red Internet y sus respectivas recomendaciones para evitar ser victimas de dichas amenazas:

- Anállsis en el puerto: los intrusos de la red Internet utilizan herramientas de análisis para buscar en los computadores que están conectados a una red en busca de puertos que estén activados o abiertos. Dichos intrusos de la red Internet comparan esta información con las vulnerabilidades conocidas de la seguridad para ver si pueden obtener acceso a los computadores identificados.

  Cómo tratar de reducir la amenaza: activar únicamente los servicios que se necesitan y utilizar la conversión de dirección de red para evitar que las direcciones estén a disposición del público en Internet.

- Negación de Servicio (DoS.- Deny Of Service): diseñado para negar el acceso a los recursos de computación o interconexión al sobrecargar al computador o la red con solicitudes continuas. Es decir que los ataques DoS envían más solicitudes de lo que la máquina o red pueden manejar.

  Cómo tratar de reducir la amenaza: se debe asegurar de que los servidores en la red de perímetro no funcionen al límite de su capacidad y que utilicen algunos métodos de seguridad en la red Internet para evitar que los paquetes falsificados entren en la red de perímetro. Además, actualizar todos los computadores y servidores con soluciones de seguridad.

- Falsificación de la dirección del Protocolo de Internet (IP - Internet Protocol): los intrusos de la red encuentran una dirección IP confiable y la modifican para que parezca que proviene de un computador confiable cuando en realidad no es así.

  Cómo tratar de reducir la amenaza: configurar los ruteadores para rechazar todo paquete que ingrese y afirme haberse originado en un computador de la red interna. De esta manera, la máquina externa no puede aprovecharse de las relaciones de confianza de la red interna.

- Monitoreo de la dirección en el Protocolo de Internet: los intrusos potenciales husmean o monitorean una red para captar información valiosa, como las direcciones IP, los nombres de usuario y las contraseñas mientras los usuarios registran un sistema remoto.

  Cómo tratar de reducir la amenaza: se debe hacer obligatorio el uso de una contraseña y el uso de los servidores proxy y NAT para reducir el monitoreo de la dirección IP.

- Virus, Caballos de Troya y Gusanos: aunque son diferentes, cada uno de estos programas maliciosos puede tener un efecto devastador en las computadoras de alguna empresa y posiblemente en toda la red.

  Virus: es un programa que se reproduce a sí mismo, accesando a otros programas en la máquina, y transfiriéndose a otras máquinas cuando el programa se envía a través de la red.

  Caballos de Troya: el término Caballo de Troya es un término general que se aplica a un rango de amenazas de códigos mal intencionados; como su nombre lo indica, un Caballo de Troya se instala por si mismo en una máquina destruyendo datos; a veces, se enmascara como otro programa que existe en el sistema y otras, crea identificadores de usuario y contraseñas; se difunden disfrazados de programas útiles. Por ejemplo, cualquier usuario puede recibir una nueva versión de algún programa favorito, y en realidad no es tal, sino que se trata de un virus que se hace pasar por un programa útil para que se lo ejecute. Para evitar ser engañado con estos virus, se debe desconfiar de nuevas versiones mejoradas de los programas que no provengan del sitio oficial de la compañía que lo genera.

  Gusanos (Worms): un gusano es un programa similar al virus, pero que a diferencia de éste no requiere infectar a otro programa, ya que se difunde en forma autónoma de computadora a computadora. En noviembre de 1988, un estudiante

norteamericano de la Universidad de Cornell, descubrió un pequeño error en un programa para rutear correos electrónicos por toda la Red, aprovechó el error y diseñó un gusano que se copiaba de servidor en servidor, burlando así la seguridad. El Gusano se distribuyó por Internet en pocas horas, causando caos en la mayoría de los grandes sistemas y dejando inactivos los centros de cómputos de casi todas las universidades y centros del gobierno de los Estados Unidos. Dos días después comenzó a repararse el daño, que costó millones de dólares y que demostró cuán frágil era la seguridad de los sistemas en ese entonces.

Cómo tratar de reducir la amenaza: siempre ejecutar el software antivirus con un archivo actualizado de definiciones de virus y nunca ejecutar un programa no solicitado sin primero ensayarlo en un computador de prueba aislado. En el caso de alguna empresa, se debe capacitar a todos los empleados para que tengan cuidado al abrir correo electrónico sospechoso que provenga de fuentes desconocidas.

I.3 PROTEGERSE DE AMENAZAS Y ATAQUES EN LA RED INTERNET

Internet es una red abierta conformada por millones de ordenadores y de personas que pueden accesar a estos sistemas. La accesibilidad y la globalidad que engrandecen Internet le convierten a su vez en objeto de amenazas y ataques que en algunos casos afectan directamente a los usuarios de la red.

Diversos sistemas criptográficos han sido desarrollados a lo largo de la historia. Sólo un grupo reducido de esos sistemas son considerados realmente seguros en la actualidad. El auge de las redes y la proliferación de servicios a través de éstas ha ejercido presión en el área de la criptografía, en demanda de tecnologías que garanticen altos niveles de seguridad.

La tecnología esencial en todas las redes automáticas y las aplicaciones de seguridad es el cifrado; del cual existen dos técnicas: cifrado convencional, también conocido como cifrado simétrico, y cifrado con clave pública, también conocido como cifrado asimétrico.

Una forma de mejorar la seguridad en el envío de información es la utilizada por los protocolos de Internet versión 4 y 6 (IPv4 e IPv6), también llamada seguridad con el protocolo de Internet (IPsec – Internet Protocol Security), y también la llamada encriptamiento, los cuales proporcionan mecanismos de autentificación y confidencialidad.

Para protegerse de posibles amenazas y ataques en una red de Internet se puede dividir en varias estrategias, algunas de ellas son:

- Crear un entorno de red seguro: existen métodos para la supervisión de los usuarios y de lo que se puede hacer en un sistema, el control de acceso, la autentificación, el uso de encriptamiento, tarjetas inteligentes, etc,.

- Cifrar los datos: un problema de las redes es que un intruso puede interceptar un sistema y robar sus datos. Esto se puede evitar no sólo utilizando diversos métodos que impidan las intercepciones, sino también cifrando la información de forma que, aunque sea robada o interceptada, no pueda ser leída.

- Aplicar técnicas de seguridad en los módem: un módem puede ser un medio de entrada ilegal a un sistema si alguien averiguara sus códigos y contraseñas. Pueden implementarse técnicas para frustrar los accesos ilegales a través de módem.

- Desarrollar planes de contingencia: si hay sólidos planes de contingencia, medidas de copias de seguridad y otras formas de manejar desastres, es más fácil recuperarse de una calamidad que esté relacionada.

- Planificar y administrar sistemas considerando la seguridad como un elemento importante: es importante planificar y administrar la red de forma apropiada para estar preparados frente a cualquier posible amenaza contra la seguridad en la red.

- Llevar a cabo una confidencialidad: proteger la información para que nadie pueda leerla o copiarla, sin la autorización del propietario. Este tipo de seguridad no sólo protege toda la información en su conjunto sino también protege cada pedazo de información, pedazos que en sí mismos pueden parecer que no hacen ningún daño pero que pueden usarse para dañar otra información confidencial.

- Crear integridad de datos: proteger la información (incluyendo programas) para evitar que se borre o altere de cualquier manera, sin el permiso del dueño de la información. Los archivos de información que deben protegerse incluyen registros contables, cintas de respaldo, hora de creación de los archivos y la documentación.

- Disponibilidad: proteger los servicios para que no se degraden o dejen de estar disponibles sin autorización. Si el sistema no está disponible cuando un usuario con autorización lo necesita, la consecuencia puede ser tan dañina como perder información que esté guardada en el sistema.

- Tener una consistencia en el comportamiento de los dispositivos de red y máquina: asegurar que el sistema se comporte como lo esperan los usuarios autorizados. Si los programas, la red, o el equipo repentinamente se comportan en forma radicalmente distinta a como lo hacían antes, en especial después de una actualización o de la eliminación de un error, puede suceder un desastre. Este tipo de seguridad también puede considerarse como asegurar que los datos y los programas que se usan sean los correctos.

- Llevar a cabo un control: reglamentar el acceso al sistema; si individuos o programas desconocidos y no autorizados están en un sistema, puede presentarse un gran problema. Hay que preocuparse de cómo entraron, qué habrán podido hacer y quién

más habrá entrado al sistema. La recuperación de un evento de esta naturaleza puede requerir mucho tiempo y dinero para reconstruir y reinstalar el sistema, verificar que no se haya cambiado o divulgado algo importante, aunque en realidad no haya pasado nada.

I.4 TIPOS DE ATAQUES A LAS REDES

Las cuatro categorías generales de ataques en una red Internet son las siguientes:

- INTERRUPCIÓN: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.
- INTERCEPCIÓN: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son interceptar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).
- MODIFICACIÓN: una entidad no autorizada no sólo consigue accesar a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- AUTENTICIDAD: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir registros a un archivo.

➢ ATAQUES PASIVOS

Los ataques pasivos, llamados a veces escuchas, suponen el intento de obtener información relativa a una comunicación. Las agresiones pasivas son del tipo de las escuchas, o monitorizaciones de las transmisiones; el propósito del oponente es obtener información que esta siendo transmitida. Existen dos tipos de agresiones en los ataques pasivos: divulgación del contenido de un mensaje y análisis del tráfico. Una conversación telefónica, un mensaje de correo electrónico, un fichero transferido puede contener información sensible o confidencial. Así, sería deseable prevenir que el oponente se entere del contenido de estas transmisiones.

Supóngase que se tiene un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes.

El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados.

Los ataques pasivos son muy difíciles de detectar ya que no implican la alteración de los datos. Sin embargo, es factible prevenir el éxito de estas agresiones. Así, el método para tratar estas agresiones esta en la prevención antes que la detección.

➢ ATAQUES ACTIVOS

Los ataques activos suponen alguna modificación del flujo de datos o la creación de flujos falsos, y se subdividen en cuatro categorías:

1. Enmascaramiento

Tienen lugar cuando una entidad pretende ser otra entidad diferente. Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa. Por ejemplo, se puede captar una secuencia de autentificación y reemplazarla por otra secuencia de autentificación válida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.

2. Repetición

La repetición supone la captura pasiva de unidades de datos y su retransmisión subsecuente para producir un efecto no autorizado.

3. Modificación de mensajes

Significa que alguna porción de un mensaje legítimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo, un mensaje con un significado "permitir al ingeniero leer el fichero confidencial de cuentas" se modifica para tener el significado "permitir a la licenciada leer el fichero confidencial de cuentas".

4. Denegación de un servicio

Previene o inhibe el uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener un objetivo específico; por ejemplo, una entidad puede suprimir todos los mensajes a un destino particular (al servicio de vigilancia de seguridad). Otro tipo de denegación de servicio es la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de forma que se degrade su rendimiento.

Las agresiones activas presentan características opuestas a las agresiones pasivas. Mientras una agresión pasiva es difícil de detectar, existen medidas disponibles para prevenirlas. Por otro lado, es bastante difícil prevenir una agresión activa, ya que para hacerlo se requeriría protección física constante de todos los recursos y de todas las rutas de comunicación. Por lo que la meta es detectarlas y

recuperarse de cualquier perturbación o retardo causado por ellas. La detección tiene un efecto convincente, también puede contribuir a la prevención.

La figura I.1 nos muestra los tipos de agresiones en que se dividen los ataques mencionados anteriormente.

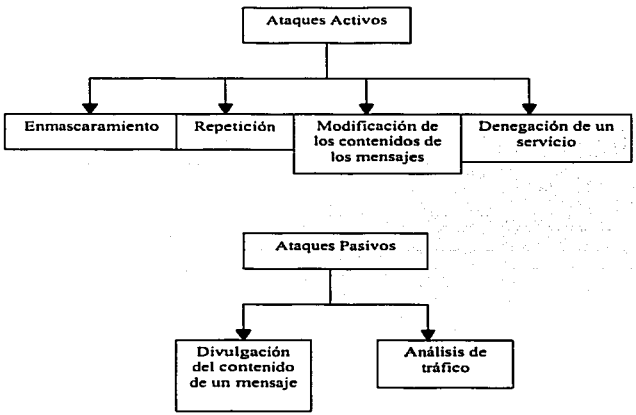


Figura I.1 Agresiones activas y pasivas a la seguridad de red.

I.5 EL PROTOCOLO DE INTERNET

El Protocolo de Internet (IP.- Internet Protocol), ha sido el fundamento de Internet y virtualmente de todas las redes privadas de múltiples suministradores. El protocolo de Internet versión 4 (IPv4) esta alcanzando el fin de su vida útil, y se ha definido un nuevo protocolo conocido como protocolo de Internet versión 6 (IPv6), para que en última instancia pueda reemplazar a IPv4.

El principal motivo que ha conducido a la adopción de una nueva versión ha sido la limitación impuesta por el campo de dirección de 32 bits en IPv4. Con un campo de dirección de 32 bits, en un principio se era posible asignar 2^{32} direcciones diferentes, alrededor de 4 000 millones de direcciones posibles. Se pensó que este número de direcciones era más adecuado para satisfacer las necesidades en Internet.

La versión 4 del Protocolo de Internet (IPv4) provee los mecanismos básicos de comunicación de la norma TCP/IP e Internet. IPv4 se ha mantenido casi sin cambios desde su adopción a finales de los 70's. Su duración ha probado su diseño flexible y poderoso. Desde el diseño de IPv4 el desempeño de los procesadores se ha incrementado en más de 2 órdenes de magnitud. Los tamaños típicos de memoria, como ya se menciono, se incremento en un factor de 32, así como el ancho de banda de la red pilar (backbone) de Internet aumento en un factor de 800. El número de servidores conectados a Internet alcanzó casi los 6 millones.

Sin embargo, a finales de la década de los 80's comenzó a haber problemas con esta versión de IP (IPv4), que empezó a manifestarse a comienzos de la década de los 90's. Algunas de las razones por las que es inadecuado utilizar estas direcciones de 32 bits son las siguientes:

- Cuando se le asigna un número de red a una red, todos los números del computador (host) de ese número de red se asignan a esa red; el espacio de direcciones para esa red podría estar poco usado, pero en lo que concierne a la efectividad del

espacio de direcciones, si se usa un número de red entonces se consumen todas las direcciones dentro de la red.

- El modelo de direccionamiento de IP requiere que se asigne un número de red único a cada red IP independientemente si la red está realmente conectada a Internet.

- Las redes están en constante crecimiento rápidamente. La mayoría de los organismos establecen redes de área local múltiples. Las redes inalámbricas están adquiriendo un mayor protagonismo. Internet ha crecido durante años.

- El uso creciente de TCP/IP en áreas nuevas producirá un crecimiento rápido en la demanda de direcciones únicas IP; como por ejemplo: el uso de TCP/IP para interconectar terminales electrónicas de puntos de venta y para los receptores de televisión por cable.

- Normalmente se le asigna una dirección única a cada computador. Una disposición más flexible es permitir múltiples direcciones IP a cada computador, esto incrementa la demanda de direcciones IP.

Una de las razones más importantes para actualizar IPv4 es la inminente saturación del espacio de direcciones. Se requiere soportar nuevas aplicaciones (videoconferencia, multimedios, etc). Se requieren mecanismos de seguridad para autentificar el emisor de un datagrama.

Por lo tanto, la necesidad de un incremento en el espacio de direcciones ha puesto la necesidad de una nueva versión de IP, ya que IP, es un protocolo viejo y se han definido nuevos requisitos en las áreas de configuración de red, flexibilidad en el encaminamiento y facilidades para el tráfico.

Algunas de las principales mejoras de IPv6 sobre IPv4 son las siguientes:

- Amplio espacio de direcciones: IPv6 utiliza direcciones de 128 bits en lugar de las direcciones de 32 bits de IPv4; por lo que supone un incremento del espacio de direcciones por un factor de 2^{96}. Esto permite espacios de direcciones del orden de 6 x 10^{23} y si la asignación de las direcciones fuera muy ineficiente, este espacio de direcciones es seguro.

- Mejora del mecanismo de opciones: las opciones de IPv6 se encuentran en cabeceras opcionales separadas, situadas entre la cabecera IPv6 y la cabecera de la capa de transporte. Esto simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los paquetes IPv6 en comparación a los datagramas IPv4, por lo que es también más fácil incorporar opciones adicionales.

- Direcciones de auto-configuración: la capacidad de direcciones de 128 bits proporciona una asignación dinámica de direcciones IPv6.

- Aumento de flexibilidad en el direccionamiento: IPv6 incluye el concepto de una dirección monodistribución (anycast), mediante la cual un paquete se entrega sólo a un nodo seleccionado de entre un conjunto de nodos. Se mejora la escalabilidad del encaminamiento multidistribución con la incorporación de un campo de acción a las direcciones multidistribución.

- Facilidad para la asignación de recursos: IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el cual el emisor solicita un tratamiento especial. Esto ayuda al tratamiento del tráfico especializado como el de video en tiempo real.

Lógicamente, el cambio de IPv4 a IPv6 no se produjo de manera repentina, ya que se tuvo que transformar toda la red a IPv6. La mayoría de los sistemas que soportan la pila de protocolos IPv6, soportan también la pila de protocolos IPv4.

Estos sistemas de pilas duales pueden existir por mucho tiempo, hasta que la mayoría de las aplicaciones implementen IPv6, el problema ahora suscita en lograr que funcionen juntos. En realidad, el incremento de tamaño de la dirección tiene poco efecto en la pila de protocolos. Los protocolos que utiliza Internet principalmente son UDP y TCP, y éstos están incluidos en el paquete IP. Cuando se envía un mensaje desde un cliente IPv4 a un servidor de pila dual, la pila respondería correctamente, pero cuando se quite la envoltura IP aparecerá un mensaje UDP o TCP según corresponda. Si esto se tiene en cuenta al programar las aplicaciones, se puede actualizar de IPv4 a IPv6 muy fácilmente.

Esencialmente, IPv4 es un subconjunto de IPv6, éste mismo, heredo todas las características buenas de IPv4 y desecho las anticuadas. Las direcciones de IPv4 son reasignadas a una dirección de IPv6. Para asignar la dirección, todos los bits superiores se establecen a cero y los últimos 48 bits son 0xFFFF seguidos de la dirección IPv4. La principal limitación, obviamente, es que no puede funcionar al revés; es decir, una aplicación IPv4 no puede aceptar directamente un paquete IPv6.

Una vez conocidas las ventajas y las limitaciones, sólo nos queda cambiar los programas de IPv4 y actualizar el núcleo y las herramientas de red para que soporten IPv6.

IPv6 permite tres tipos de direcciones, los cuales son:

1. Unidistribución (unicast): es un identificador para una interfaz individual; un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.

2. Monodistribución (anycast): es un identificador para un conjunto de interfaces, normalmente pertenecientes a diferentes nodos. Un paquete enviado a una dirección monodistribución se entrega a una de las interfaces identificadas por esa dirección, la más cercana, de acuerdo a la medida de distancia del protocolo de encaminamiento.

3. Multidistribución (multicast): es un identificador para un conjunto de interfaces, normalmente pertenecientes a diferentes nodos. Un paquete enviado a una dirección multidistribución se entrega a todas las interfaces identificadas por esa dirección.

I.6 FUNCIONES DE DISPERSIÓN

Los sistemas de encriptamiento de clave publica generalmente encriptan de forma mucho más lenta que los sistemas de encriptamiento de clave privada, como el estándar de encriptamiento de datos (DES – Data Encryption Standar) por ejemplo. También los esquemas de firma digital suelen ser muy lentos y, en ocasiones, la longitud de la firma suele ser similar o mayor que el propio menaje que se firma. La necesidad de firmar mensajes, es el hecho no deseable de que la longitud de la firma sea extensa, hace pensar en la conveniencia de buscar una solución a este problema. Esta solución consiste en utilizar las llamadas funciones de dispersión antes de firmar un mensaje.

Una función de dispersión también se le conoce como función hash o función resumen; y es una función computable que se aplica a un mensaje m de tamaño variable, una representación de tamaño fijo del propio mensaje: H(m) se pude reducir a 128 bits o 64 bits.

Por otra parte, estas funciones de dispersión también pueden utilizarse para determinar el resumen de un documento y hacer publico dicho resumen, sin revelar el contenido del documento del que procede el mensaje.

Una vez dada la definición de lo que es una función de dispersión, el problema señalado respecto a la longitud de la firma digital se resuelve si en lugar de firmar el mensaje completo m se firma el resumen del mensaje, esto es, se firma H(m).

De esta manera, un usuario A que desee enviar el mensaje m a un usuario B, junto con su firma, lo que hará será enviar el mensaje m encriptado, es decir, enviará $c = f_b(m)$, y como firma enviará la contraseña, obtenida a partir del resumen H(m), encriptada.

De esta forma, el usuario B se asegura de que, en efecto, es A quien le envía el mensaje y de que el mensaje corresponde con el enviado por A. Si la comprobación anterior no fuera correcta, B debe rechazar el mensaje, ya sea por que la firma digital de A ha sido falsificada, o por que el mensaje ha sido manipulado.

La elección de una función de dispersión para ser utilizada a la hora de firmar digitalmente mensajes debería llevarse a cabo de modo que sea lo suficientemente segura para su uso criptográfico. Así, debería ser difícil encontrar un mensaje m cuyo resumen sea de un valor dado, si no fuera de este modo, un escucha podría sustituir el mensaje firmado por un mensaje falso. Además, también debería ser difícil poder encontrar dos mensajes distintos que proporcionen el mismo resumen, por otra parte, la longitud del resumen debería ser lo suficientemente larga como para evitar una investigación exhaustiva a un escucha. Por ejemplo, si una función de dispersión proporciona un resumen de 100 bits, la investigación exhaustiva debería llevar, al menos, 2^{100} intentos para conseguir igualar un valor dado, y aproximadamente 2^{50} intentos, por lo menos, para producir dos entradas con el mismo resumen.

Con lo que se acaba de mencionar, el ataque contra una firma digital puede llevarse a cabo por dos medios. El primero consiste en atacar el procedimiento matemático en el que se basa el método de la firma, y el segundo atacar la función de dispersión utilizada para crear el resumen del mensaje. Por lo tanto, es aconsejable

elegir un método para firmar digitalmente y una función de dispersión que requieran esfuerzos comparables para ser rotos.

Las funciones de dispersión más utilizadas con propósitos criptográficos son las funciones MD2, MD4 y MD5 (MD.- Message Digest – Mensaje Resumen), estas funciones producen resúmenes de 128 bits, y el único ataque que se conoce contra ellas es el de la investigación exhaustiva.

A continuación se da una breve explicación de las funciones de dispersión mencionadas:

- MD2: diseñado para ordenadores con procesador de 8 bits. Todavía se usa, pero no es recomendable, debido a su lentitud de proceso.

- MD4: desarrollado por Ron Rivest, uno de los fundadores de clave pública con clave variable. Aunque se considera un sistema inseguro, es importante porque ha servido de base para la creación de otras funciones de dispersión. Un sistema de ataque desarrollado por Hans Dobbertin posibilita el crear mensajes aleatorios con los mismos valores de dispersión (colisiones), por lo que ya no se usa. De hecho, existe un algoritmo que encuentra una colisión en segundos.

- MD5: también obra de Ron Rivest, que se creó para dar seguridad a MD4, y que ha sido ampliamente usado en diversos campos, como autenticador de mensajes en el protocolo de la capa de socket segura (SSL – security Socket Layer) y como firmador de mensajes en el programa de correo llamado muy buena privacidad (PGP – Pretty Good Privacy). Si embargo, fue roto con un sistema de ataque en 1996 por el mismo investigador que lo hizo con MD4, el señor Dobbertin, que consiguió crear colisiones en el sistema MD5, aunque por medio de ataques parciales. Pero lo peor es que también consiguió realizar ataques que comprometían la no-colisión, por lo que se podían obtener mensajes con igual dispersión que otro determinado. A pesar de todo esto, MD5 se sigue usando bastante en la actualidad.

El resultado de aplicar una función resumen a un texto es un número grande, el número resumen, que tiene las siguientes características:

- Todos los números resumen generados con un mismo método tienen el mismo tamaño sea cual sea el texto utilizado como base.
- Dado un texto base, es fácil y rápido para un ordenador calcular su número resumen.
- Es imposible reconstruir el texto base a partir del número resumen.
- Es imposible que dos textos base diferentes tengan el mismo número resumen.

Las funciones de dispersión y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los certificados digitales. Para que una función pueda considerarse como función de dispersión debe cumplir los siguientes aspectos:

- Debe transformar un texto de longitud variable en un bloque de longitud fija, que generalmente es pequeña (algunas son de 16 bits).
- Debe ser cómoda de usar e implementar.
- Debe ser irreversible, es decir, no se puede obtener el texto original del resumen de dispersión.
- Debe ser imposible encontrar dos mensajes diferentes cuya firma digital mediante la función de dispersión sea la misma (no-colisión).
- Si se desea además mantener un intercambio de información con confidencialidad, basta con cifrar el documento a enviar con la clave pública del receptor.

CAPITULO II
SEGURIDAD CON CIFRADO Y FIRMAS

Las condiciones para intercambiar información con diferentes destinos se parecen mas a un viaje en la vía publica que a un viaje en un automóvil blindado y con los vidrios polarizados. Es decir el intercambio de información permite ver diferentes tipos de cosas como su Protocolo de Internet (IP), así como el destino. Asimismo, es importante tener en cuenta que el intercambiar información es casi tan seguro como enviar una postal por el correo tradicional, salvo que el destino utilice algunos métodos de protección como el cifrado. Este método de protección de información es más efectivo que las regulaciones gubernamentales, ya que no permite que los sitios obtengan la información en primer lugar en vez de confiar en las reglamentaciones gubernamentales, que son reactivas y es posible que no se hagan cumplir. Los usuarios no sólo pueden montarse en un automóvil blindado (utilizando cifrado), sino que además pueden ponerse pelucas, máscaras y bigotes, lo cual les permite ocultar su identidad mejor de lo que pueden hacerlo en el mundo externo.

El cifrado consiste en transformar un texto en claro (inteligible por todos) mediante un mecanismo de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Se distinguen dos métodos generales de cifrado: asimétrico y convencional.

Cifrado Convencional

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el sistema encriptado es simétrico o de clave secreta. Estos sistemas son mucho más rápidos que los de clave asimétrica, y resultan apropiados para el cifrado de grandes volúmenes de datos. Ésta es la opción utilizada para cifrar el cuerpo del mensaje.

Cifrado asimétrico

Por otro lado, cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el sistema encriptado es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada ni descifrar el texto con ella cifrado. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales, como se explicará posteriormente.

II.1 CIFRADO CONVENCIONAL

El cifrado convencional, también llamado cifrado simétrico o de clave única, era el único tipo de cifrado en uso antes de la introducción del cifrado de clave pública a finales de la década de los 70's. El cifrado convencional ha sido utilizado para las comunicaciones secretas por incontables individuos y grupos, desde Julio Cesar con el intercambio de cada letra del alfabeto por aquella que distaba un número fijo de posiciones a izquierda o derecha dentro del mismo hasta la fuerza Alemana de los U-boat y actualmente los diplomáticos, militares y los comerciantes. Es todavía el cifrado más utilizado mundialmente de los dos tipos de cifrado.

Un esquema de cifrado convencional tiene cinco elementos:

- Texto nativo (plaintext): es el mensaje original o datos que actúan como entrada al algoritmo de cifrado.
- Algoritmo de cifrado: el algoritmo descifrado lleva a cabo varias substituciones y transformaciones en el texto nativo.

- Clave secreta: la clave secreta es también la entrada al algoritmo de cifrado. Las substituciones y transformaciones exactas realizadas por el algoritmo dependen de la clave.
- Texto cifrado: es el mensaje aleatorio que se produce en la salida. Depende del texto nativo y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.
- Algoritmo de descifrado: es esencialmente el algoritmo descifrado ejecutado al revés. Toma como entradas el texto cifrado y la clave secreta y produce el texto nativo de salida (original).

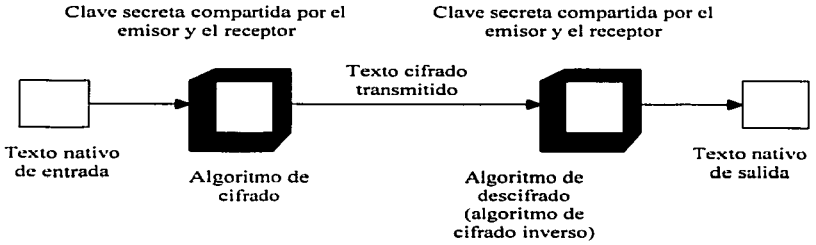


Figura II.1-Modelo simplificado del cifrado convencional.

Existen dos requisitos para la utilización segura del cifrado convencional:

1. Se necesita un algoritmo de cifrado robusto. Como mínimo, es de desear un algoritmo tal que si el intruso conoce el algoritmo y tiene acceso a más de un texto cifrado, sea incapaz de descifrar el texto o adivinar la clave. Este requisito se puede enunciar de una forma más estricta; el oponente debería de ser incapaz de descifrar

el texto o descubrir la clave incluso si posee un determinado número de texto cifrados junto a los textos nativos que producen cada texto cifrado.

2. El emisor y el receptor deben haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y conoce el algoritmo, todas las comunicaciones que utilicen esta clave pueden ser leídas.

Existen dos enfoques generales para atacar el esquema de cifrado convencional. El primer ataque se conoce como criptoanálisis. El ataque de criptoanálisis se basa en la naturaleza del algoritmo más algún conocimiento de las características generales del texto nativo o incluso de algunos pares texto nativo-texto cifrado. Este tipo de ataque explota las características del algoritmo para intentar deducir un texto nativo especifico o deducir la clave que se esta utilizando. Si el ataque tiene éxito en deducir la clave, el efecto es catastrófico: todos los mensajes cifrados antiguos y futuros con esa clave están en peligro de ser modificados.

El segundo método, conocido como fuerza bruta, es intentar cada clave posible en un trozo de texto cifrado hasta que se obtenga una traducción inteligible del texto nativo. La tabla II.1 nos muestra cuanto tiempo se necesita para el caso de varios tamaños de clave. La tabla muestra loa resultados para cada tamaño de clave, suponiendo que se tarda 1 µs. en llevar a cabo un único descifrado, que es un orden de magnitud razonable para los computadores de hoy en día. Con el uso de una arquitectura paralela masiva de microcomputadores, seria posible alcanzar velocidades de procesamientote varias ordenes de magnitudes superiores. La última columna de la tabla considera los resultados de un sistema que pudiera procesar 1 millón de claves por microsegundo. Como se pude ver, a este nivel de rendimiento, ya no se puede considerar computacionalmente segura una clave de 56 bits.

Tamaño de la clave (bits)	Numero de claves alternativas	Tiempo necesario a 1 cifrado/ μs	Tiempo necesario a 10^6 cifrados/ μs
32	2^{32}=4,3 x 10	2^{31}μs=35,8 minutos	2,15 milisegundos
56	2^{56}=7,2 x 10	2^{56}μs=1.142 años	10,01 horas
128	2^{128}=3,4 x 10	2^{127}μs=5,4x10 años	5,4 x 10^{18} años
168	2^{168}= 3,7 x 10	2^{167}μs= 5,9 x 10años	5,9 x 10^{30} años

Tabla II.1 Tiempo promedio necesario para una búsqueda de clave.

II.1.1 Localización de los dispositivos de cifrado.

El enfoque más potente y más común en contra de los ataques a la seguridad de red es el cifrado. Si se va a utilizar el cifrado en contra de estas amenazas, entonces se necesita decidir que se va a cifrar y a donde se va a situar el algoritmo de cifrado. Como muestra la figura II.2 hay dos alternativas fundamentales: cifrado de enlace y cifrado extremo-a-extremo.

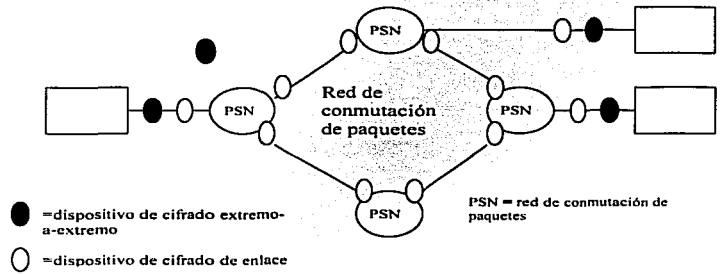


Figura II.2 Cifrado a través de una red de conmutación de paquetes.

Con el cifrado de enlace, cada enlace de comunicación vulnerable se equipa en ambos extremos con un dispositivo de cifrado. Así, todo el tráfico a través de los enlaces de comunicaciones se protege. Aunque esto requiere de muchos dispositivos de cifrado en redes grandes, el valor de esta opción está claro. Una desventaja es que el mensaje debe ser descifrado cada vez que entra un paquete a la red de conmutación; esto es así ya que el conmutador debe leer la dirección (numero de circuito virtual) en la cabecera del paquete para encaminarlo, ya conociendo la clave, de esta forma, el mensaje es vulnerable en cada nodo, ya que después de leerlo lo encamina el mensaje descifrado. Si la red es de conmutación de paquetes publica, el usuario no tiene control sobre la seguridad en los nodos.

Con un cifrado extremo-a-extremo, el proceso de cifrado se realiza en los dos sistemas finales. El dispositivo origen cifra los datos. Los datos cifrados se transmiten sin alterarlos a través de la red hasta el computador o terminal destino. El destino comparte una clave con el origen y es, por lo tanto, capaz de descifrar los datos. Esta técnica protege la transmisión contra agresiones en los enlaces o conmutadores de red.

Considere el siguiente ejemplo. Un conmutador se conecta a una red de conmutación de paquetes, establece un circuito virtual a otro computador y se prepara para enviar datos al dicho computador utilizando un cifrado extremo-a-extremo. Los datos se transmiten por esa red en forma de paquetes, que constan de una cabecera y algunos datos de usuario. Supongamos que el computador cifra el paquete entero, incluyendo la cabecera. Esto no funcionara ya que, solo el otro computador puede descifrar el paquete. El nodo de conmutación recibirá el paquete cifrado y no será capaz de leer la cabecera. Por lo tanto, no será capaz de encaminar el paquete. De esto se concluye que el computador solo debe cifrar la parte de datos de usuario y no la parte de cabecera, para que esta pueda ser leída por la red.

Así, con el cifrado extremo-a-extremo los datos de usuario están seguros. Sin embargo, el modelo de trafico no lo esta, ya que las cabeceras de los paquetes se transmiten sin cifrarlas. Para alcanzar un mayor grado de seguridad, se necesita cifrado de enlace y cifrado de extremo-a-extremo,

Para concluir, cuando se utilizan ambas formas, el computador cifra parte de datos de usuario usando una clave de cifrado extremo-a-extremo. Después se cifra el paquete entero usando una clave de cifrado de enlace. Conforme el paquete viaja por la red, cada nodo conmutador descifra el paquete utilizando una clave de cifrado de enlace para poder leer la cabecera y luego cifra de nuevo el paquete entero para enviarlo al siguiente enlace. Ahora el paquete esta seguro excepto durante el tiempo en el que el paquete esta en la memoria del nodo de conmutación, en el que la cabecera esta desprotegida.

II.1.2 Mecanismo de seguridad específico

Los mecanismos de seguridad son el tercer aspecto que se considera en la seguridad de la información. Cabe recordar que el primer aspecto es el ataque de seguridad y el segundo los servicios de seguridad.

Un mecanismo de seguridad es una técnica que se utiliza para implementar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad. Los mecanismos de seguridad implementan varios servicios básicos de seguridad o combinaciones de estos servicios básicos. Los servicios de seguridad especifican qué controles son requeridos y los mecanismos de seguridad especifican cómo deben ser ejecutados los controles.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los diferentes servicios de seguridad. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

No existe un único mecanismo capaz de proveer todos los servicios, sin embargo, la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información. Los mecanismos pueden ser clasificados como preventivos, detectivos, y recuperables.

Los mecanismos de seguridad pueden tener dos categorías:

1. Mecanismos de seguridad generalizados.
2. Mecanismos de seguridad específicos

El relleno de tráfico es un mecanismo considerado dentro de los mecanismos de seguridad específicos, ya que estos definen la implementación de servicios concretos.

El relleno de tráfico es un mecanismo que provee una generación de tráfico falso, esto se logra enviando por la red mensajes sin contenido (basura) para obtener un flujo constante de mensajes, un tráfico constante o la longitud del mensaje constante, esto

significa que se envía tráfico falso junto con los datos válidos, esto es de gran valía ya que en una situación en la que haya necesidad de mantener un vasto intercambio de información entre nodos que regularmente apenas si tienen alguna comunicación ocasional, el incremento de actividad en el canal podría entonces ser motivo de un análisis de tráfico por parte de atacantes. Para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo, se inyecta tráfico sin información en las redes para confundir a los observadores de la red.

El relleno de tráfico es una función que produce salida de texto cifrado continuamente, incluso en ausencia de texto nativo. Se genera un flujo de datos aleatorio continuamente. Cuando hay disponible texto nativo, se cifra y se transmite. Cuando el texto nativo no está presente, los datos aleatorios se cifran y transmiten. Esto hace imposible que un agresor distinga entre flujo de datos verdaderos y basura y por tanto le resulta imposible deducir la cantidad de trafico.

II.1.3 Distribución de claves

Para que funcione el cifrado convencional, las dos partes que intercambian datos deben tener la misma clave y ésta debe ser protegida para que no la conozcan las otras partes. Además, es deseable realizar normalmente cambios de la clave para limitar la cantidad de datos comprometidos si un agresor aprende la clave. Por lo tanto, la potencia de cualquier sistema de cifrado se apoya en una técnica de distribución de claves, que se refiere a los medios para distribuir una clave a dos partes que quieran intercambiar datos, impidiendo que otras vean la clave. La distribución de claves se puede conseguir de varias formas. Para dos partes A y B:

1. A puede seleccionar una clave y entregarla físicamente a B.
2. Una tercera parte selecciona la clave y la entrega físicamente a A y B.
3. Si A y B utilizado previamente y recientemente una clave, una de las partes podría transmitir la nueva clave a la otra cifrada utilizando la clave previa.

4. Si A y B tienen cada uno una conexión cifrada con una tercera parte C, ésta podría entregar una clave a través de los enlaces cifrados a A y B

Las opciones 1 y 2 exigen una entrega manual de una clave. Este es un requisito razonable para el cifrado de enlace ya que cada dispositivo de cifrado de enlace solo va intercambiar datos con su pareja en el otro extremo de enlace. Sin embargo, para cifrado extremo-a-extremo, la entrega manual es difícil. En un sistema distribuido, cualquier terminal o computador se ve envuelto en intercambios con muchos otros terminales o computadores durante mucho tiempo. Así, cada dispositivo necesita varias claves, suministradas dinámicamente. El problema es especialmente difícil en sistemas distribuidos a través de una gran área.

La opción 3 es una posibilidad valida tanto para el cifrado de enlace como el de extremo-a-extremo, pero si un agresor tiene el éxito al conseguir una clave, las siguientes claves serán reveladas. Incluso si se hacen cambios frecuentes en la clave de cifrado de enlace, estos se deberían de hacer manualmente. La opción 4 es la preferible para proporcionar claves de cifrado extremo-a-extremo. La figura II.3 muestra una implementación que cumple con la opción 4 para el cifrado extremo-a-extremo. En la figura se ha ignorado el cifrado de enlace. Esta se puede incorporar, o no, según se requiera. Para este esquema, se identifican estas dos claves:

- Clave de sesión: cuando dos sistemas finales (computadoras, terminales, etc.) desean comunicarse, establecen una comunicación lógica (por ejemplo, circuitos virtuales). Durante la duración de la conexión lógica, todos los datos de usuario se cifran con una clave de sesión de un solo uso. Al terminar la sesión, o conexión, la clave de sesión se destruye.
- Clave permanente: es la clave usada entre entidades con el objetivo de distribución de claves de sesión.

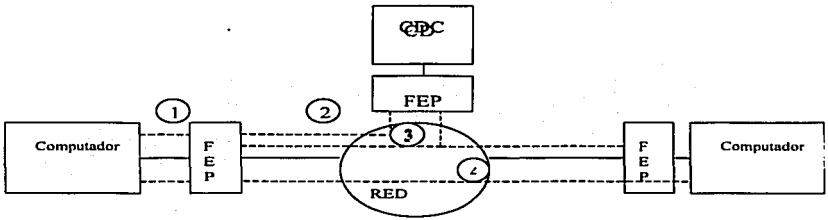


Figura II.3 Distribución de claves automática para protocolos orientados a conexión.

FEP: Procesador frontal
CDC: Centro de distribución de claves

1. Computador envía un paquete solicitando conexión
2. El procesador frontal almacena los paquetes, solicita a CDC una clave de sesión
3. CDC distribuye la clave de sesión a ambos procesadores frontales
4. Los paquetes almacenados se transmiten

II. 2 CIFRADO DE CLAVE PRIVADA

En criptografía existen dos tipos muy diferentes de algoritmos de cifrado: los algoritmos de cifrado de clave privada y los algoritmos de cifrado de clave pública.

Los primeros, han sido utilizados desde los principios de la historia de la criptografía y se basan en la idea de tener una clave secreta que sirve para cifrar y descifrar, de ahí que a estos algoritmos también se les denomine algoritmos de clave

simétrica. Ejemplos de estos algoritmos son el conocido algoritmo César, el Estandar de Cifrado de Datos (DES - Data Encryption Standard), etc.

Cada clave privada tiene un papel especifico en el cifrado y descifrado de documentos. Se puede pensar en una clave pública como en una caja fuerte de seguridad. Cuando un remitente cifra un documento usando una clave pública, ese documento se pone en la caja fuerte, la caja se cierra, y el bloqueo de la combinación de ésta se gira varias veces. La parte correspondiente a la clave privada, esto es, el destinatario, es la combinación que puede volver a abrir la caja y retirar el documento. Dicho de otro modo, sólo la persona que posee la clave privada puede recuperar un documento cifrado usando la clave pública asociada al cifrado.

Con el ejemplo que se acaba de mencionar se ha mostrado el procedimiento de cifrar y descifrar documentos de un modo muy simple. Si el usuario quisiera cifrar un mensaje para Javier, lo haría usando la clave pública de Javier, y él lo descifraría con su propia clave privada. Si Javier quisiera enviar un mensaje al usuario, lo haría con la clave pública del usuario, y éste lo descifraría con su propia clave privada.

II.3 CIFRADO DE CLAVE PÚBLICA

El cifrado de clave publica, propuesta en público por primera vez por Diffie y Hellman en 1976 se explicará en el capitulo IV, es el primer avance realmente revolucionario en el cifrado en literalmente miles de años. Y esto es debido a una razón, el algoritmo de clave pública se basa en funciones matemáticas en lugar de sustituciones y permutaciones. Pero lo más importante, la criptografía de clave publica es asimétrica y utiliza dos claves independientes, en contraste con el cifrado simétrico convencional que solo utiliza una clave. Utilizar dos claves tiene consecuencias profundas en las áreas de privacidad, distribución de claves y autentificación.

Los sistemas de cifrado de clave pública se inventaron con el fin de evitar por completo el problema del intercambio de claves. Un sistema de cifrado de clave pública usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona. La otra clave es *privada* y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Este protocolo resuelve el problema del intercambio de claves, que es inherente a los sistemas de cifrado simétricos. No hay necesidad de que el remitente y el destinatario tengan que ponerse de acuerdo en una clave. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo *n* pares de claves por cada *n* personas que deseen comunicarse entre ellas.

Los sistemas de cifrado de clave pública se basan en funciones llamadas trampa de un sólo sentido. Una función de un sólo sentido es aquélla cuya computación es fácil, mientras que invertir la función es extremadamente difícil. Por ejemplo, es fácil multiplicar dos números primos juntos para sacar uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función-trampa de un sentido es algo parecido, pero tiene una trampa. Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso. Por ejemplo, si tenemos un número compuesto por dos factores primarios y conocemos uno de los factores, es fácil computar el segundo. Dado un cifrado de clave pública basado en factorización de números primos, la clave pública contiene un número compuesto de dos factores primos grandes, y el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. El algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos, para que el descifrado sea fácil si poseemos la clave privada que contiene uno de los factores, pero extremadamente difícil en caso contrario.

Como con los sistemas de cifrado simétricos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave. Por lo tanto el tamaño de la clave es una medida del seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el de un cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe enumerar hasta 2^{81}-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con un clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits es suficiente para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

A continuación se mencionan los malentendidos comunes que afectan al cifrado de clave pública. Un primer malentendido es que el cifrado de clave pública es mas seguro frente al criptoanálisis que el cifrado convencional. En realidad, la seguridad de cualquier esquema de cifrado depende de la longitud de la clave y el trabajo computacional que requiere romper un cifrado. No hay nada en principio del cifrado convencional o de clave publica que haga a uno superior al otro desde el punto de vista de resistir el criptoanálisis. Un segundo malentendido es que el cifrado de clave publica es una técnica de uso general que ha hecho que se quede obsoleta el cifrado convencional. Por el contrario, a causa de la computación suplementaria de los esquemas actuales de cifrado por clave pública, no es probable que el cifrado convencional sea abandonado. Finalmente, existe el parecer de que la distribución de claves es trivial cuando se utiliza cifrado de clave publica, comparado con el dialogo mas bien molesto que se requiere con los centros de distribución de claves en el cifrado convencional. De hecho, se necesita alguna forma de protocolo, a menudo implicando a un agente central, y los procedimientos implicados no son más sencillos o más eficientes que los que se requieren para el cifrado convencional.

El esquema de cifrado de clave pública tiene seis elementos:

- Texto nativo: es el mensaje legible o datos que se pasan al algoritmo de cifrado como entrada.
- Algoritmo de cifrado: el algoritmo de cifrado lleva a cabo varias operaciones aritméticas sobre el texto nativo, como en el cifrado de clave pública con clave variable.
- Clave pública y privada de los usuarios: este es el par de claves que se ha seleccionado para que una se utilice para el cifrado y la otra para el descifrado. Las transformaciones exactas que realiza el algoritmo de cifrado dependen de la clave pública o privada que se suministra como entrada.
- Texto cifrado: es el mensaje mezclado producido como salida. Depende del texto nativo y de la clave. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.
- Algoritmo de descifrado: este algoritmo acepta el texto de cifrado, la otra clave (privada) y produce el texto nativo de salida (original).

La figura II.4 muestra la transmisión de datos con cifrado y autentificación de clave pública.

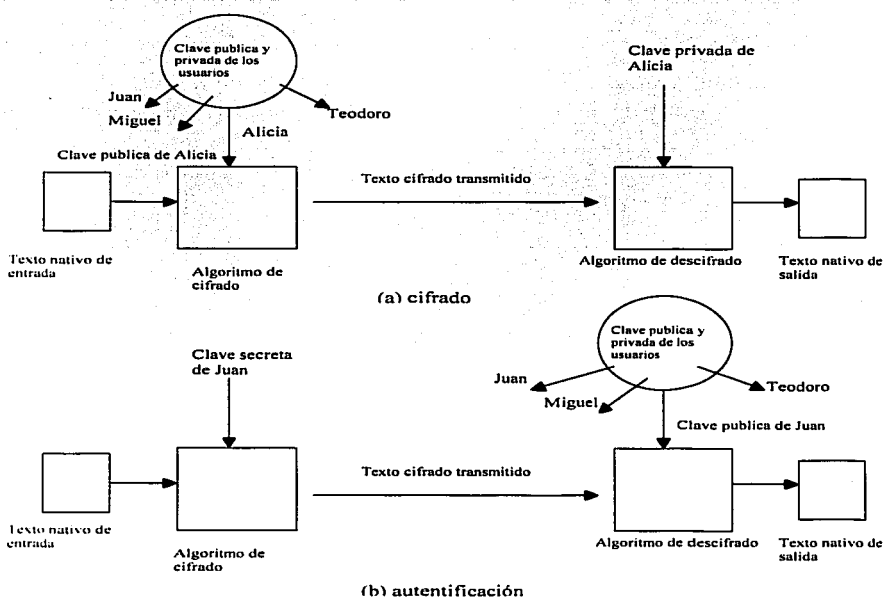


Figura II.4 Cifrado y autentificación de clave publica

Como el nombre sugiere, la clave publica se hace publica para que la utilice el resto de la gente, mientras que la clave privada solamente la conoce el dueño. Un algoritmo de criptografía de clave pública de propósito general se basa en una clave de

cifrado y en una clave diferente, pero relacionada para el descifrado. Además, estos algoritmos tienen las siguientes características importantes:

- No es factible computacionalmente determinar la clave de descifrado dado solamente el algoritmo de criptografía y la llave de cifrado.
- Para la mayoría de los esquemas de clave publica, cualquiera de las dos claves que se utilizan, se puede emplear para el cifrado y la otra para el descifrado.

Los pasos esenciales para el cifrado y descifrado son los siguientes:

1. Cada usuario genera un par de claves que se van a utilizar para el cifrado y el descifrado de los mensajes.
2. Cada usuario publica una de las dos claves de cifrado situándola en un registro o fichero publico. Esta es la clave pública. La clave compañera se mantiene privada. Cada usuario mantiene una colección de claves públicas de otros usuarios.
3. Si Juan desea enviar un mensaje privado a Alicia, el cifra el mensaje utilizando la clave publica de Alicia.
4. Cuando Alicia recibe el mensaje, lo descifra utilizando su clave privada. Ningún otro destino puede descifrar el mensaje ya que solamente Alicia conoce la clave privada de Alicia.

Con esta técnica, todos los participantes tienen acceso a las claves públicas y las claves privadas se generan localmente por cada participante y por lo tanto nunca se distribuyen. Mientras un usuario controle su clave privada, los mensajes que le llegan son seguros. Un usuario puede cambiar su clave privada en cualquier instante de tiempo y publicar la clave pública compañera para reemplazar la clave publica obsoleta.

II.4 CIFRADO DE CLAVE PUBLICA CON CLAVE VARIABLE

Existen diferentes sistemas de clave pública pero el más extendido es el RSA. Este criptosistema, creado en 1978 por Rivest Shamir y Adleman. Patentaron el algoritmo y cuando alcanzó popularidad fundaron la empresa RSA Seguridad de Datos (Data Security) para la explotación comercial. Para implementación y comercialización se deben pagar derechos a esta empresa, pero actualmente se encuentran muchas versiones gratuitas en Internet. Fuera de los EE.UU. solo se permite la utilización del algoritmo con clave menores o iguales a 512 bits.

RSA es un algoritmo de clave pública que soporta una longitud de clave variable, así como tamaño variable del bloque de texto a encriptar. La longitud común de la clave es de 512 bits. El chip más rápido para la clave pública con clave variable tiene una velocidad de proceso mayor que 600 kbps con un módulo de 512 bits, como ya se dijo anteriormente, lo que supone que puede ejecutar más de 1000 operaciones de la clave privada de RSA por segundo.

El algoritmo utiliza las siguientes claves:

- Como públicas dos números grandes elegidos por un programa: **e** y **n**.
- Como privada un número grande **d**, consecuencia de los anteriores.

El cálculo de estas claves se realiza en secreto en la máquina depositaria de la privada. Este proceso tiene mucha importancia para la posterior seguridad del sistema. El proceso es el siguiente:

- Se buscan dos números grandes (entre 100 y 300 dígitos) y primos: **p** y **q**.
- Se calcula **F**=(**p**-1)*(**q**-1) y **n**=**p***q.
- Se busca **e** como un número sin múltiplos comunes a **F**.
- Se calcula $\mathbf{d}=\mathbf{e}^{-1} \text{mod} \mathbf{F}$ (mod = resto de la división de enteros).
- Se hacen públicas las clave **n** y **e**, se guarda **d** como clave privada y se destruyen **p**, **q** y **F**.

El sistema de criptoanálisis que debería utilizarse para romper este sistema consiste en buscar la clave privada **d** a partir de la pública **e** y **n**. Para esto basta con encontrar los números **p** y **q**; éstos son la descomposición en factores primos de **n**, ya que **n=p*q**. Actualmente aún no se ha descubierto ninguna forma analítica de descomponer números grandes en factores primos.

Para entender mejor lo que es el cifrado de clave pública con clave variable, antes que nada necesitamos un sistema para convertir mensajes en números. Lo más típico es sustituir cada letra del texto por dos cifras indicando su posición en el alfabeto; es decir, cambiamos cada "a" por "01", cada "b" por "02", cada "c" por "03", etc., y de esta forma podemos convertir un importantísimo mensaje secreto como "hola" en "08151201". Debería haber alguna forma de incluir espacios y signos de puntuación, pero estos detalles no son esenciales; lo importante es que a partir de ahora los mensajes que queremos cifrar y descifrar son simplemente números.

A diferencia de otros métodos más tradicionales, en los que tanto el emisor como el receptor tienen que conocer la misma clave, en la clave pública con clave variable es el receptor quien tiene toda la clave; al emisor le deja conocer la parte pública de la clave, que sirve para cifrar mensaje. El receptor guarda muy cuidadosamente la parte privada de la clave, que sirve para descifrar.

Construir una clave es fácil. Buscamos dos números primos como 3 y 11 y hacemos dos cosas con ellos. Primero los multiplicamos para obtener 33. Luego les restamos uno, los multiplicamos, y al resultado le sumamos 1, para obtener (3-1)*(11-1)+1=21. Y a continuación (esto es nuevo) buscamos un divisor pequeño de 21, por ejemplo 3, y calculamos 21/3=7.

Ya tenemos nuestra clave: para cifrar elevamos a la potencia 3, dividimos por 33, y nos quedamos con el resto. Para descifrar, elevamos a la potencia 7, dividimos por 33, y nos quedamos con el resto. Ahora que tenemos nuestra clave, anunciamos la parte pública a todo el mundo que nos quiera mandar mensajes. Esto lo podemos hacer

poniendo nuestra clave de PGP en nuestra página Web, o con el siguiente anuncio en el periódico:

Diario El País, edición internacional
Anuncios por palabras

Soy Rubén, la clave pública con clave variable para enviarme mensajes es elevar a la potencia 3, dividir por 33, y mandarme el resto.

Por supuesto, en el anuncio no se menciona para nada el número 7, que sirve para descifrar los mensajes; ésta es la parte privada de la clave, la que guarda en secreto el receptor.

Todos los sistemas de clave pública conocidos se basan en que, de alguna forma, es posible representar la misma información de dos formas diferentes, tales que pasar de una forma a la otra es fácil, pero pasar de la otra a la una es prácticamente imposible.

En el caso de la clave pública con clave variable, en principio es lo mismo tener los números primos 3 y 11 que tener su producto, 33. Decimos "en principio" porque dados dos números es fácil multiplicarlos, y dado un número es teóricamente posible factorizarlo en producto de números primos. Todos hemos hecho esto en la escuela para simplificar quebrados.

Ahora bien, imaginemos que los números primos que hemos usado para construir nuestra clave son enormes y tienen unas cien cifras cada uno. Cualquier ordenador puede encontrar números primos así de grandes en un instante y multiplicarlos en una milésima de segundo para obtener un resultado de doscientas cifras. De hecho, el ordenador lo hace; cada vez que usted visita una página web genera sobre la marcha una nueva clave de usar y tirar. No es posible descomponer en factores primos un número con doscientas cifras, esta es la cualidad del sistema.

Sin entrar en detalles, desde el punto de vista matemático descifrar un mensaje cifrado con clave pública con clave variable es exactamente el mismo problema que

factorizar la clave (el número 33 en nuestro ejemplo). Ambas tareas son equivalentes, y si pudiésemos hacer una podríamos hacer la otra. Como "se sabe" que los números así de grandes no se pueden factorizar, el método es seguro.

II.5 FIRMAS DIGITALES.

En 1991, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST. – National Institute of Standards and Technology), hizo publico su método llamado Estandar de Firmas Digitales (DSS. – Digital Signature Standard), desarrollado por la agencia de seguridad nacional de los E.E.U.U.

El estándar de firmas digitales (DSS) no es un método de encriptamiento; es, sin embargo, un aspecto integral de criptografía. Específicamente, el DSS es propuesto como un elemento electrónico para verificar la integridad y el origen de información no clasificada. Su intención es la de facilitar papeleos y transacciones gubernamentales pero se aplica más en cualquier situación donde se requiere verificar la integridad y el origen de un mensaje. La firma digital se envía con un mensaje que autentifica al emisor.

El uso de firmas digitales es análogo a varias situaciones familiares, como lo es el de proporcionar un password o clave secreta para tener acceso a una cuenta en computadora, firmar un contrato, o cambiar un cheque. Cuando uno cobra un cheque personal monetario, usualmente se le pregunta por alguna forma de identificación. Esto lo protege de que alguien quiera falsificar la firma y utilizar su cuenta bancaria, por ejemplo. Sin embargo, cuando uno firma un contrato, alguien debe verificar la firma. Esto protege al contratista en caso de que después uno no este de acuerdo con los términos del contrato.

En principio, basta con cifrar un documento con la clave privada para obtener una firma digital segura, puesto que nadie excepto el poseedor de la clave privada puede

hacerlo. Posteriormente, cualquier persona podría descifrarlo con la clave pública, demostrándose así la identidad del firmante. En la práctica, debido a que los algoritmos de clave pública son muy ineficaces a la hora de cifrar documentos largos, los protocolos de firma digital se implementan junto con funciones unidireccionales de dispersión (hash), de manera que en vez de firmar un documento, se firma un resumen del mismo. Este mecanismo implica el cifrado, mediante la clave privada del emisor, del resumen de los datos, que serán transferidos junto con el mensaje. Éste se procesa una vez en el receptor, para verificar su integridad. Por lo tanto, los pasos del protocolo son los que se muestran en la figura II.5:

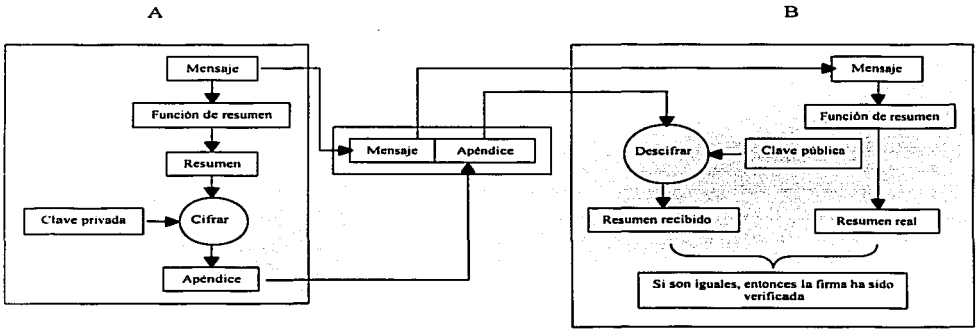


Figura II.5 Pasos del protocolo de firmas digitales.

1. A genera un resumen del documento.
2. A cifra el resumen con su clave privada, firmando por tanto el documento.
3. A envía el documento junto con el resumen firmado a B.

4. B genera un resumen del documento recibido de A, usando la misma función unidireccional de dispersión. Después descifra con la clave pública de A el resumen firmado. Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

De esta forma se ofrecen conjuntamente los servicios de no repudio, ya que nadie excepto A podría haber firmado el documento, y de autenticación, ya que si el documento viene firmado por A, podemos estar seguros de su identidad, dado que sólo él ha podido firmarlo. En último lugar, mediante la firma digital se garantiza asimismo la integridad del documento, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen que había sido firmada.

Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. El firmante cifra el documento con su clave *privada*. Cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrarla. Este algoritmo satisface las dos propiedades necesarias para una buena función de dispersión, pero en la práctica este algoritmo es demasiado lento para que sea de utilidad.

Como alternativa está el uso de funciones de dispersión designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos. Al usar uno de estos algoritmos, un documento se firma con una función dispersión, y el valor de dispersión es la firma. Otra persona puede comprobar la firma aplicando también una función de dispersión a su copia del documento y comparando el valor de dispersión resultante con el del documento original. Si concuerdan, es casi seguro que los documentos son idénticos.

Claro que el problema está en usar una función de dispersión para firmas digitales que no permita que un atacante interfiera en la comprobación de la firma. Si el documento y la firma se enviaran descifrados, un atacante podría modificar el documento y generar una firma correspondiente sin que lo supiera el destinatario. Si sólo se cifrara el documento, un atacante podría manipular la firma y hacer que la

comprobación de ésta fallara. Una tercera opción es usar un sistema de clave pública híbrido para cifrar tanto la firma como el documento. El firmante usa su clave pública, y cualquiera puede usar su clave pública para comprobar la firma y el documento. Esto suena bien, pero en realidad no tiene sentido. Si este algoritmo hiciera el documento seguro también lo aseguraría de manipulaciones, y no habría necesidad de firmarlo. El problema más serio es que esto no protege de manipulaciones ni a la firma, ni al documento. Con este algoritmo, sólo la clave de sesión del sistema de cifrado simétrico, es cifrada usando la clave privada del firmante. Cualquiera puede usar la clave pública y recuperar la clave de sesión. Por lo tanto, es sencillo para un atacante recuperar la clave de sesión y usarla para cifrar documentos substitutos y firmas para enviarlas a terceros en nombre del remitente.

Un algoritmo que funciona es aquél que hace uso de un algoritmo de clave pública para cifrar sólo la firma. En particular, el valor de dispersión se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público. Si el documento se modifica, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone que debe descubrir. El DSA es un algoritmo de firmado de clave pública que funciona como hemos descrito.

El cifrado de clave pública se puede utilizar de otra forma. Suponga que Juan quiere enviar un mensaje a Alicia y, aunque no es importante que el mensaje se mantenga secreto, quiere que Alicia este segura que en realidad el mensaje es de el. En este caso. Juan utiliza su propia clave privada. Cuando Alicia recibe el texto cifrado, encuentra que puede descifrarlo con la clave pública de Juan, demostrando así que el mensaje ha sido cifrado por Juan. Nadie más tiene la clave privada de Juan y, por lo tanto, nadie mas ha podido crear el texto cifrado que se descifra con la clave privada de Juan. De esta forma, el mensaje cifrado completo sirve como firma digital. Además, es imposible alterar el mensaje sin acceder a la clave privada de Juan, por lo tanto el mensaje esta autentificado en términos de la fuente y de integridad de los datos.

En el esquema precedente, se cifra en mensaje entero, lo que, aunque valida al autor y al contenido, requiere de una gran cantidad de almacenamiento. Cada documento se debe guardare en texto nativo para ser útil por motivos prácticos. Se debe guardar también una copia del texto cifrado para que se pueda verificar el origen y el contenido en caso de disputa. Una forma más eficiente de conseguir el mismo resultado es cifrar un bloque pequeño de bits que sea una función del documento. Este bloque, llamado autentificador, debe tener la propiedad de que no sea factible cambiar el documento sin cambiar el autentificador. Si el autentificador se cifra con la clave privada del emisor, sirve como una firma que verifica al origen, el contenido y el secuenciamiento.

Es importante enfatizar que el proceso de cifrado que se acaba de describir no proporciona privacidad. Esto es, el mensaje que se envía esta seguro frente alteraciones, pero no lo esta de ser escuchado. Esto es obvio en el caso de una firma basada en una parte del mensaje, ya que el resto del mensaje no esta cifrado. Incluso en el caso de cifrar el mensaje entero, no hay protección de confidencialidad ya que cualquier observador puede descifrar el mensaje utilizando la clave pública del emisor.

II.5.1 Gestión de claves

Una buena gestión de claves es crucial para asegurarse, no sólo de la integridad de nuestros ficheros de claves, sino también de la integridad de los anillos de claves de otros. El punto central en la gestión de claves es la noción que hay detrás de firmar las claves. Firmar las claves tiene dos propósitos principales: nos permite detectar una manipulación en nuestros anillos de claves, y nos permite certificar que una clave realmente pertenece a la persona cuyo nombre aparece en el identificador de usuario de la clave. Las firmas de las claves también se usan en un esquema conocido como anillo de confianza para hacer extensiva la certificación de claves que no han sido firmadas directamente por el usuario, sino que han sido firmadas por otros en los que él confía.

Un par de claves se compone de una clave pública y otra privada. Una clave pública se compone de la parte pública de la clave de firmado maestra, las partes públicas de las subclaves de firmado y cifrado, y de un juego de identificadores de usuario que se usa para asociar la clave pública con una persona real. Cada una de estas partes contiene datos sobre sí misma. Para una clave estos datos constan de su propio identificador, fecha de creación, fecha de caducidad, etc... Para un identificador de usuario, estos datos constan del nombre de la persona a la que identifica, un comentario opcional, y una dirección de correo electrónico. La estructura de las claves privadas es parecida, con la diferencia de que sólo contiene las partes privadas de las claves, y que no tiene la información del identificador de usuario.

Con el cifrado convencional, un requisito fundamental para dos entes que se comunican de una forma segura es que compartan una clave secreta. Supóngase que Juan quiere crear una aplicación para enviar mensajes que el permitirá intercambiar correo electrónico de una forma asegura con cualquiera que tenga acceso a Internet o alguna otra red que los dos comparten. Supóngase que Juan quiere hacer esto utilizando solo cifrado convencional. Con el cifrado convencional, Juan y su corresponsal, digamos, Alicia, deben presentar una forma para compartir la clave secreta única y que nadie más conoce. Si Alicia se encuentra cerca de Juan, Juan pude generar la clave y escribirla en un papel o almacenarla en un disquete y dársela a Alicia. Pero si Alicia se encuentra en otra parte del continente o del mundo. Podría cifrar la clave utilizando cifrado convencional y enviarla por correo electrónico a Alicia, pero esto significa que Juan y Alicia deben compartir una clave secreta para poder cifrar esta nueva clave secreta.

Por lo tanto Juan y cualquiera que utilice este nuevo paquete de correo electrónico se deben de enfrentar al mismo problema con cualquier corresponsal potencial. Cada par de corresponsales deben compartir una clave secreta única.

El mayor problema para utilizar cifrado convencional es como distribuir las claves secretas de una forma segura. Este problema se elimina con el cifrado de clave pública por el simple hecho de que la clave privada nunca se distribuye. Si Juan quiere

establecer correspondencia con Alicia u otra persona, genera un único par de claves, una privada y otra publica. Guarda la clave privada de una forma segura y difunde la clave pública a todos y cada uno. Si Alicia hace lo mismo, entonces Juan tiene la clave pública de Alicia, Alicia tiene la clave publica de Juan y ay pueden comunicarse con seguridad. Cuando Juan desea comunicarse con Alicia, puede hacer lo siguiente:

1. Preparar un mensaje.
2. Cifrar el mensaje utilizando cifrado convencional con una clave de sesión convencional.
3. Cifrar la clave de sesión utilizando cifrado de clave publica con la clave pública de Alicia.
4. Incorporar la clave de sesión cifrada al mensaje y enviarlo a Alicia.

Solamente Alicia es capaz de descifrar la clave de sesión y por tanto de recuperar el mensaje original.

Es justo señalar, sin embargo, que se ha reemplazado un problema por otro. La clave privada de Alicia es segura ya que no necesita revelarla nunca; sin embargo, Juan debe estar seguro de que la clave pública con el nombre de Alicia escrita en ella es de hecho la clave pública de Alicia. Alguien podría haber difundido una clave publica y haber dicho que era la de Alicia. La forma común de solucionar este problema es ingeniosa: utilizar cifrado de clave pública para autentificar claves públicas. Esto supone la existencia de alguna autoridad o individuo señalado y de confianza que actué como sigue:

1. Alicia genera una clave pública y la envia a la autoridad para certificarla.
2. La autoridad determina por algún procedimiento, como una entrevista personal, que esta es la autentica clave pública de Alicia.
3. La autoridad incorpora una marca de tiempo a la clave pública, genera un código de dispersión al resultado y cifra el resultado con su clave privada formando una firma.
4. La firma se incorpora a la clave pública.

Cualquiera equipado con una copia de la clave publica de X puede ahora verificar que la clave publica de Alicia es autentica.

II.5.2 Autoridades emisoras de certificados

Entidad encargada de establecer y avalar la autenticidad de las claves públicas pertenecientes a los usuarios (entidades finales) u otras entidades emisoras de certificados. Entre las actividades de una entidad emisora de certificados están enlazar claves públicas a nombres distinguidos mediante certificados firmados, administrar los números de serie de los certificados y revocar certificados. La entidad emisora de certificados se llama también CA.

Los certificados contienen información que se utiliza al establecer identidades en una red, un proceso llamado autenticación. De forma similar a los métodos convencionales de identificación, los certificados permiten a los servidores y usuarios Web autenticarse entre si antes de establecer una conexión. Los certificados también contienen valores de cifrado, o *claves*, que se utilizan al establecer una conexión entre el cliente y el servidor. La información, como el número de una tarjeta de crédito, que se envía a través de esta conexión está cifrada de forma que personas no autorizadas. no puedan interceptarla ni utilizarla.

Puede obtener un certificado de cliente de una organización comercial en la que se confía mutuamente, llamada entidad emisora de certificados. Antes de emitir un certificado, la entidad emisora necesita que le proporcione información de identificación, como un nombre, una dirección y el nombre de la organización. El alcance de esta información puede variar según los requisitos de garantía de identificación del certificado. Si necesita un certificado para proporcionar una garantía absoluta acerca de su identidad, la entidad emisora de certificados necesitará mucha más información acerca de usted; la recopilación de esta información puede requerir una entrevista personal con la entidad emisora y el refrendo de un notario.

Existen 3 tipos de entidades emisoras de certificados:

- Entidad emisora de certificados con autofirma. En una entidad emisora de certificados con autofirma, la clave pública del certificado y la clave utilizada para comprobar el certificado son la misma.
- Entidad emisora de certificados subordinada. En una entidad emisora de certificados subordinada, la clave pública del certificado y la utilizada para comprobar los certificados son diferentes. Este proceso, donde una entidad emite un certificado a otra entidad emisora, se conoce como certificación cruzada.
- Entidad emisora de certificados raíz. El cliente confía plenamente en una entidad emisora de certificados raíz, que ocupa la posición más alta en una jerarquía de certificados. Todas las cadenas de certificados terminan en una entidad emisora de certificados raíz. La entidad raíz debe firmar su propio certificado porque no existe ninguna entidad emisora de certificados superior en la jerarquía de certificados.

Todas las entidades emisoras de certificados con auto-firma son entidades raíz, ya que la cadena de certificados termina cuando se alcanza una entidad emisora de certificados con auto-firmas.

CAPÍTULO III
SEGURIDAD CON EL PROTOCOLO DE INTERNET

Si se tuviera que enumerar las principales características de Internet, se podría decir, que en primer lugar, es una red totalmente abierta y pública, sin ningún tipo de jerarquía establecida ni de autoridad central. El número de usuarios aumenta día con día de manera espectacular, así como el tipo de operaciones realizadas. Se puede decir que la red Internet no es más que una red general formada por la interconexión de multitud de redes.

Con lo dicho anteriormente, es fácil imaginar la inseguridad de los datos transmitidos y almacenados en los computadores conectados. En las distintas capas del modelo Internet se pueden establecer diferentes controles de seguridad atendiendo al tipo de los datos. En el nivel de el protocolo de Internet, se tiene que establecer un modelo de seguridad que controle los paquetes que circulan por la red; los servicios de seguridad que se pueden proporcionar son: autenticación, integridad, confidencialidad y control de acceso. Así también, se tiene que atender la seguridad en las aplicaciones; es decir, la seguridad de los datos de los usuarios; también es necesario atender la seguridad global del sistema terminal y su entorno local.

El protocolo IPv6 ha sido diseñado prestando una atención especial a dichos aspectos de seguridad. Algunos de los elementos de seguridad introducidos en las definiciones de IPv6 han sido tomados e implementados en IPv4.

Desde 1992, existe un grupo de trabajo denominado Grupo de Ingeniería en Internet (IETF - Internet Engineering Task Force), en el cual la seguridad con el protocolo de Internet (IPsec – Internet Protocol Security), es el encargado de la normalización del Protocolo de Seguridad del Protocolo de Internet (IPSP – Internet Protocol Security Protocol) y del Protocolo de Gestión de Claves para Internet (IKMP - Internet Key Management Protocol). Aunque en un principio estos trabajos fueron dirigidos a crear la arquitectura de seguridad que debían incorporar el IPv6, también han adaptado esta arquitectura al IPv4.

Seguridad con el Protocolo de Internet (IPsec - Internet Protocol Security) es un conjunto de recomendaciones y protocolos definidos para proteger intercambios de datos sobre IP, mediante encriptación al nivel de red, lo que permite proveer un servicio de seguridad de extremo a extremo. Este servicio permite la autenticación, integridad, control de acceso, y confidencialidad. Seguridad con el Protocolo de Internet provee servicios similares a la capa de socket segura (SSL - Secure Sockets Layer), pero al nivel de redes, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto. Es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de seguridad con el protocolo de Internet para poder usarlo. Se puede usar cualquier protocolo IP sobre IPsec. Se pueden crear túneles cifrados (Redes Privadas Virtuales), o simple cifrado entre computadoras (ordenadores). Debido a que dispone de tantas opciones, seguridad con el protocolo de Internet es más bien complejo. Seguridad con el Protocolo de Internet se puede usar como túnel de tráfico para conexiones de redes privadas virtuales (VPN – Virtual Private Networks). Sin embargo, su utilidad va más allá de las redes privadas virtuales. Con un registro central de intercambio de claves de Internet (IKE - Internet Key Exchange), cada máquina en Internet podría comunicarse con otra y usar cifrado y autenticación de alto grado.

Los protocolos de seguridad con el Protocolo de Internet pueden suministrar el control de acceso, autenticación, integridad de datos y confidencialidad para cada paquete IP entre dos nodos de red. Seguridad con el Protocolo de Internet puede ser utilizado por dos computadores, por una pasarela y un computador, o por dos pasarelas.

IPv4 ha sido usado durante casi 20 años con problemas. El problema más grave es que el espacio de direcciones IPv4 disponible para conectar nuevos nodos a Internet se esta acabando, especialmente si se considera las nuevas perspectivas de uso que se están implementando como lo puede ser conexiones a celulares, o incluso artefactos del hogar. IPv6 soluciona este problema y agrega una gran cantidad de mejoras, orientadas a los actuales usos que se le dan a Internet (en particular transmisiones multimediales y de tiempo real), así como mejoras en el ruteo y la autoconfiguración de

redes. Puede ser instalado como una actualización normal de software de dispositivos de Internet y puede interoperar con IPv4. Suministrando una plataforma para las nuevas funcionalidades que se requerirán en el futuro. Se espera que IPv6 gradualmente reemplace a IPv4, coexistiendo ambos algunos años durante un periodo de transición.

III.1 ASOCIACIONES DE SEGURIDAD

Seguridad con el Protocolo de Internet utiliza dos protocolos de seguridad en IP, los cuales son: Cabecera de Autenticación (AH – Authentication Header, RFC 2402), y Carga Útil de Seguridad Encapsulada (ESP – Encapsulating Security Payload, RFC 2406).

➢ Cabecera de Autenticación (AH – Authentication Header)

El funcionamiento de la cabecera de autenticación es el de proporcionar integridad en falta de conexión, permite asegurar la autenticación del origen de los datos, así como la integridad de los paquetes IP durante la transmisión. La cabecera de autenticación no encripta los datos, pero cualquier modificación en los datos que se envían puede ser detectado. La confidencialidad de los datos no está contemplada. En pocas palabras, la cabecera de autenticación permite autenticar el origen de datos e incluir servicios de integridad.

Dado que algunos campos en la cabecera del paquete pueden variar durante la transmisión, es necesario calcular los datos que permiten la autenticidad del paquete sobre una copia del mismo en la que los campos susceptibles de modificación estén puestos a cero. Sobre esta copia modificada se aplica el algoritmo criptográfico correspondiente.

A pesar de que los mecanismos para generar la Cabecera de Autenticación pueden implementarse en las pasarelas (gateways), es mucho más recomendable hacerlo a nivel de usuarios para dar la máxima seguridad.

- **Carga Útil de Seguridad Encapsulada (ESP – Encapsulating Security Payload)**

El funcionamiento de la carga útil de seguridad encapsulada es el de proporcionar confidencialidad a través de la encripción de la carga útil; es decir, es un mecanismo para proporcionar confidencialidad y actuar sobre los datos del paquete IP cifrándolos y encapsulándolos. El control de acceso es proporcionado a través del uso y manejo de los métodos para el control del flujo de tráfico. En pocas palabras, la carga útil de seguridad encapsulada proporciona servicio de confidencialidad en los datos. En el formato del paquete de datos encapsulados aparecen varios campos:

- Campo con el índice de SPI.
- Datos del paquete IP.
- Datos aleatorios de relleno para ajustar la longitud del nuevo paquete.
- Campo con la longitud de los datos de relleno.
- Campo para indicar el protocolo del campo de datos del paquete IP.

En el campo de datos del paquete IP pueden incluirse solamente los datos procedentes de la capa de transporte, funcionamiento en modo transporte; o el paquete IP completo, funcionamiento en modo túnel.

Tan pronto como se han establecido las asociaciones de seguridad, los terminales pueden intercambiar datos de forma segura. Las asociaciones de seguridad tienen un periodo de validez de una hora a partir del momento en que se transfiere el último paquete. Por ello, si los terminales necesitan comunicarse entre sí después de haber caducado la asociación de seguridad, tendrán que establecer una asociación de seguridad nueva. El periodo de validez predeterminado de las asociaciones de

seguridad se puede eliminar o modificar en el caso de que se considere inadecuado. Por ejemplo, las asociaciones de seguridad de los servidores de alta seguridad deben caducar a los pocos minutos de recibirse el último paquete.

Un concepto muy importante que aparece tanto en los mecanismos de autentificación como de privacidad en el protocolo de Internet es la asociación de seguridad (SA - Security Association). Una asociación es la relación en un solo sentido entre un emisor y un receptor que proporciona servicios de seguridad al tráfico que se transporta. Si se necesita una relación paritaria, para un intercambio seguro en dos sentidos, entonces se requieren dos asociaciones de seguridad. Los servicios de seguridad se proporcionan a una asociación de seguridad para que utilice cabecera de autenticación o carga útil de seguridad encapsulada, ambos pueden utilizarse conjuntamente. Una asociación de seguridad está identificada por tres parámetros:

1. Un Índice de Parámetros de Seguridad (SPI – Security Parameters Index): es una cadena de bits asignada a dicha asociación de seguridad y solamente con un significado local. El SPI se transporta en las cabeceras AH y SPI para permitir que el sistema receptor seleccione la asociación de seguridad bajo la que se procesaran los paquetes recibidos.

2. Dirección IP destino: actualmente sólo se permiten direcciones monodistribución; esta es la dirección del sistema final del destino de la asociación de seguridad, que puede ser un usuario final o un sistema de red.

3. Identificador del Protocolo de Seguridad: esto indica si la asociación es una asociación de seguridad AH o ESP.

En cualquier paquete IP, la asociación de seguridad está univocamente identificada por la dirección destino en la cabecera IPv4 o IPv6 y el SPI incluida en la cabecera de extensión (AH o ESP).

Una implementación de seguridad con el protocolo de Internet incluye una base de datos de asociaciones de seguridad que define los parámetros asociados con cada asociación de seguridad. Una asociación de seguridad se define normalmente por los siguientes parámetros:

- Contador de número de secuencia: un valor de 32 bits utilizado para generar el campo número de secuencia en las cabeceras AH o ESP.

- Desbordamiento del contador de secuencia: un indicador que avisa si se debe generar un evento audible si se produce un desbordamiento del contador de números de secuencia y así prevenir de transmisiones de paquetes adicionales de la asociación de seguridad.

- Ventana de anti-repeticiones: utilizada para determinar si un paquete AH o ESP que llega es una repetición, mediante la definición de una ventana deslizante dentro de la cual se tiene que encontrar el número de secuencia.

- Información AH: algoritmo de autentificación, claves, tiempos de vida de las claves y parámetros relacionados que se utilizan con AH.

- Información ESP: algoritmos de cifrado y autentificación, claves, valores de inicialización, tiempos de vida de las claves y parámetros relacionados que se utilizan con ESP.

- Tiempo de vida de la Asociación de Seguridad: un intervalo de tiempo o contador de bytes después del cual una asociación de seguridad se tiene que reemplazar por una asociación de seguridad nueva, y por lo tanto un nuevo índice de parámetros de seguridad.

- Modo de Protocolo IPsec: modo túnel, modo transporte o marca de ambos, necesario en todas las implementaciones; dichos modos se describirán más adelante.

- Unidad de Transferencia Máxima del camino: cualquier unidad de transferencia máxima (MTU – Maxim Transfer Unit) observada en el camino, es decir, el tamaño máximo de los paquetes que se pueden transmitir sin fragmentación; y variables de caducidad (necesario en todas las implementaciones).

Las Asociaciones de Seguridad se trata de convenios entre dos o más partes para decidir tanto sobre los servicios de seguridad que van a utilizar como sobre el proveedor de estos servicios. Los acuerdos a los que llegan las partes implicadas se transmiten como un conjunto de parámetros de seguridad, entre los que se encuentran los siguientes:

- Parámetros de autenticación para la cabecera de autenticación (algoritmo, claves, etc.,).
- Parámetros de confidencialidad para la carga útil de seguridad encapsulada (algoritmo, claves, etc.,).
- Parámetros de las claves en la asociación de seguridad (período de validez).
- Dirección fuente de la asociación de seguridad.
- Nivel de seguridad de los datos protegidos.

Para comprobar que el receptor de un mensaje pertenece a una asociación de seguridad (SA – Security Association) determinada, en caso contrario no podrá autenticar ni descifrar el mensaje, se utiliza una palabra de 32 bits cuyo valor se negocia durante el proceso de gestión de claves. Este valor recibe el nombre de índice de parámetros de seguridad (SPI – Security Parameters Index). El SPI, junto con la dirección de destino, forman el identificador de una asociación de seguridad.

Las claves de sesión que se pueden utilizar en el protocolo de seguridad IP son de tres tipos:

1. Una clave de sesión única entre computadores.
2. Una clave de sesión para usuarios.
3. Una clave de sesión por aplicación.

III.2 MODO TRANSPORTE

El modo transporte proporciona protección principalmente a los protocolos de las capas superiores. Algunos ejemplos incluyen a segmentos del Protocolo de Control de Transmisión (TCP - Transmisión Control Protocol) o Protocolo de Servicios de Datagrama (UDP - User Datagram Protocol) o paquetes del Protocolo de Control para Mensajes de Internet (ICMP - Internet Control Message Protocol) que operan directamente encima de IP en la pila de protocolos de un computador. Normalmente el modo transporte se utiliza en comunicaciones extremo a extremo entre dos computadores, por ejemplo: un cliente y un servidor o dos estaciones de trabajo. Cuando ambos computadores implementan la cabecera de autenticación o la carga útil de seguridad encapsulada sobre IPv4, la carga útil son los datos que siguen a la cabecera IP. Para IPv6, la carga útil son los datos que siguen a la cabecera IP y a cualquier cabecera de extensión que esté presente, con la posible excepción de la cabecera de las opciones para el destino, que se podría incluir en la protección. La carga útil de seguridad encapsulada en modo transporte cifra y opcionalmente autentifica la carga útil de IP pero no la cabecera IP. La cabecera de autenticación en modo transporte autentifica la carga útil de IP y porciones seleccionadas de la cabecera IP.

La figura III.1 ejemplifica la transmisión de datos en modo transporte.

Figura III.1 Modo transporte

En el modo transporte es el computador el que genera los paquetes, solo se encriptan los datos y la cabecera permanece intacta, añade pocos bytes, y permite ver las direcciones de origen y destino.

III.3 MODO TÚNEL

El modo túnel proporciona protección al paquete IP entero. Para poder llevar a cabo esto, después de que los campos de la cabecera de autenticación o de la carga útil de seguridad encapsulada se han incorporado al paquete IP, el paquete entero más un campo de seguridad se tratan como la carga útil de un paquete IP exterior nuevo con una cabecera IP exterior nueva. El paquete original entero o interior, viaja a través del túnel desde un punto de la red IP a otro punto, ningún dispositivo de encaminamiento a lo largo del camino es capaz de examinar la cabecera IP interior. Ya que el paquete original esta encapsulado, un paquete más grande podría tener direcciones origen y destino totalmente diferentes, añadiendo seguridad. El modo túnel se utiliza cuando uno o ambos extremos de una asociación de seguridad es una pasarela de seguridad, como lo es un dispositivo de encaminamiento que implementa IPsec. Con el modo túnel, un determinado número de computadores en la red y detrás del dispositivo pueden estar

implicados en comunicaciones seguras sin implementar seguridad con el protocolo de Internet. Los paquetes no protegidos generados por tales computadores se transmiten mediante un túnel a través de redes externas mediante una asociación de seguridad en modo túnel establecidas por el software IPsec en el dispositivo de encaminamiento seguro en las fronteras de la red local. La carga útil de seguridad encapsulada en modo túnel cifra y opcionalmente autentifica al paquete IP interior completo, incluyendo la cabecera IP interior. La cabecera de autenticación en modo túnel autentifica el paquete IP interior completo y porciones seleccionadas de la cabecera IP exterior.

La figura III.2 ejemplifica la transmisión de datos en modo túnel.

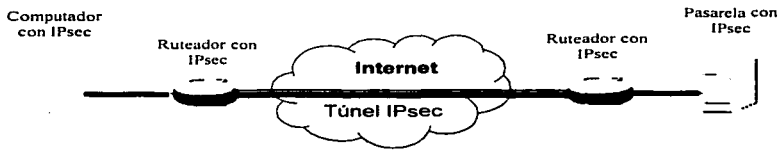


Figura III.2 Modo túnel

En el modo túnel uno de los extremos de la comunicación es una pasarela, se encripta el paquete IP entero, y para el sistema final los datos llegan completos.

El uso de la cabecera de la carga útil de seguridad encapsulada proporciona privacidad e integridad de los datos de los paquetes IP. Dependiendo de los requisitos del usuario, este mecanismo se puede utilizar para encriptar bien el segmento de la capa de transporte (por ejemplo, TCP, UDP, ICMP), conocido como modo de transporte de la carga útil de seguridad encapsulada o bien el paquete IP completo, conocido como túnel de la carga útil de seguridad encapsulada.

La cabecera de la carga útil de seguridad encapsulada comienza con el valor SPI de 32 bits que identifica la asociación de seguridad. El resto de la cabecera puede contener parámetros del algoritmo de cifrado que se esta empleando. Parte de esta cabecera será transmitida en claro y parte cifrada.

El modo transporte de la carga útil de seguridad encapsulada se utiliza para encriptar datos transportados por IP. Normalmente, estos datos son un segmento de la capa de transporte, como segmentos TCP o UDP, que a su vez contienen datos de la capa de aplicación. El funcionamiento es el siguiente:

En el origen, el bloque de datos que consta de la parte final (la que va encriptada) de la cabecera de la carga útil de seguridad encapsulada más el segmento entero de la capa de transporte, se encriptan y se reemplaza el texto original por el encriptado. El paquete es entonces encaminado al destino. Los nodos intermedios no necesitan saber el contenido encriptado.

El nodo destino examina y procesa la cabecera IP más cualquier cabecera adicional. Obtiene el índice de parámetros de seguridad de la cabecera de la carga útil de seguridad encapsulada y junto con la dirección destino determina la asociación de seguridad con la que desencriptar la información.

En el modo túnel de la carga útil de seguridad encapsulada se utiliza para encriptar el paquete IP completo. Para este modo, la carga útil de seguridad encapsulada se incorpora como prefijo al paquete y después, el paquete más una parte final de la cabecera, se encripta. Mediante este método es imposible realizar un análisis del tráfico.

Como los datos de encaminamiento (dirección destino y opciones diversas) van encriptados es imposible transmitir el paquete tal cual. Para ello se encapsula en otro paquete IP con la información necesaria para realizar el encaminamiento pero no con información que sirva para analizar el tráfico.

III.4 GESTIÓN DE CLAVES

Las asociaciones de seguridad necesitan compartir claves que sólo deben conocer los miembros legítimos de una determinada asociación de seguridad. Cuando el número de usuarios es elevado, se necesitan protocolos de gestión de claves eficientes que garanticen la seguridad en la distribución de las claves a todos los usuarios. También hay que tener en cuenta la revocación de las claves obsoletas. Con este fin, seguridad con el protocolo de Internet ha desarrollado el Protocolo de Gestión de Claves para Internet (IKMP – Internet Key Management Protocol).

Anteriormente se llevaron a cabo algunas propuestas,. entre dichas propuestas destacaron:

- El Protocolo de Gestión de Claves Modular (MKMP – Modular Key Management Protocol) de IBM.
- Gestión de Claves Simples para el Protocolo de Internet (SKIP – Simple Key Management for Internet Protocol), de Sun.
- Asociación de Seguridad de Internet Y Protocolo de Gestión de Claves (ISAKMP – Internet Security Association and Key Management Protocol) propuesto por la Asociación de Seguridad Nacional (NSA – National Security Association).
- Protocolo de intercambio de claves llamado OAKLEY, de la universidad de Arizona.

La porción de gestión de claves de seguridad con el protocolo de Internet supone la determinación y distribución de claves secretas. Los documentos de la arquitectura de seguridad con el protocolo de Internet obligan a permitir dos tipos de gestión de claves:

- Manual: un administrador del sistema configura manualmente cada sistema con sus propias claves y con las claves de otros sistemas de comunicación. Esto es práctico para entornos pequeños y relativamente estáticos.

- Automática: un sistema automático habilita la creación bajo demanda de claves para la asociación de seguridad y facilita el uso de claves en sistemas distribuidos grandes con una configuración cambiante. Un sistema automático es lo más flexible pero requiere más esfuerzos para configurar y requiere de más software. Por lo tanto, es más probable que las instalaciones más pequeñas opten por una gestión de clave manual.

El protocolo de gestión de claves automático que se utiliza en seguridad con el protocolo de Internet se conoce como ISAKMP/Oakley, que consta de los siguientes elementos:

- Protocolo de determinación de claves Oakley: Oakley es un protocolo de intercambio de claves basado en el algoritmo Diffie-Hellman, pero proporcionando una seguridad adicional. En particular, el algoritmo Diffie-Hellman sólo no autentifica a los dos usuarios que intercambian claves, haciendo el protocolo vulnerable a la suplantación. Oakley incluye mecanismos para autentificar a los usuarios.

- Asociación de Seguridad de Internet y Protocolo de Gestión de Claves (ISAKMP - Internet Security Association and Key Management Protocol): proporciona un entorno de trabajo para la gestión de claves en Internet y proporciona el soporte del protocolo específico, incluyendo formatos, para la negación de los atributos de seguridad.

ISAKMP por sí mismo no impone un algoritmo de intercambio de claves específico; sino consiste de un conjunto de tipos de mensajes que permiten el uso de una variedad de algoritmos de intercambio de claves. Oakley es el algoritmo de intercambio de claves de uso obligatorio en la versión inicial de ISAKMP.

ISAKMP/Oakley es el protocolo estándar para realizar una asociación de seguridad entre el emisor y el receptor, como se muestra en la figura III.3; durante un intercambio de ISAKMP/Oakley, las dos máquinas acuerdan los métodos de autenticación y seguridad de datos, realizan una autenticación mutua y después

generan una clave compartida para la codificación de datos subsecuente. Antes de que los datos sean intercambiados de forma segura se debe iniciar una negociación entre las partes para determinar la asociación de seguridad que van a usar, o lo que es lo mismo, los parámetros de seguridad que se van a usar.

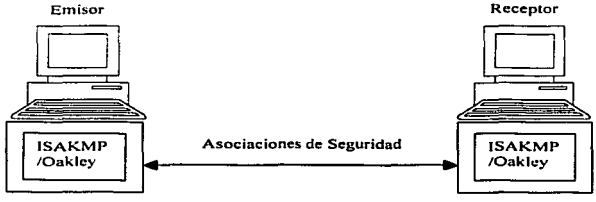


Figura III.3 Intercambio del protocolo ISAKMP/Oakley entre dos computadores para llevar a cabo una asociación de seguridad.

Para esta negociación se utiliza el protocolo ISAKMP/Oakley. El ISAKMP centraliza la administración de las asociaciones de seguridad y el Oakley genera y administra las claves usadas para proteger la información.

ISAKMP/Oakley funciona en dos fases diferentes. La primera fase se dedica a establecer un canal seguro entre ambos interlocutores, generando una asociación de seguridad denominada ISAKMP Asociación de Seguridad. En definitiva son los parámetros de seguridad que se van a usar en este protocolo.

Una vez establecida esta fase, se negocian las asociaciones de seguridad necesarias, en la segunda fase. En la primera fase se producen los pasos siguientes:

1. Negociación de la política.

Son cuatro parámetros obligatorios que son parte indiscutible de la ISAKMP Asociación de Seguridad:

- Algoritmo de encriptado (DES-CBC, 3DES, 40-bit DES).
- Función de dispersión (MD5 o SHA).
- Método de autenticación (Certificado, clave compartida o sistemas de distribución de claves).
- Algoritmo Diffie-Hellman para la generación de claves.

2. Intercambio de claves.

Se realiza el intercambio de claves. Una vez realizado este intercambio ambas partes generaran una clave que tan solo ellos conocen y que usaran para el encriptado de la información, incluido el siguiente paso de esta primera fase.

3. Autenticación.

Se usa la clave generada en el paso anterior junto con los algoritmos y métodos especificados en la primera fase para autenticar a cada extremo de la comunicación.

El iniciador ISAKMP presenta una oferta de Asociación de Seguridad a su interlocutor. El que contesta puede aceptar la propuesta tal y como está u ofrecer una respuesta con alternativas.

En la segunda fase se negocia la asociación de seguridad necesaria para realizar la comunicación. Y sus pasos son:

a) Negociación de la política

Debe definir lo siguiente:

- Protocolo a usar, Cabecera de Autenticación o Carga Útil de Seguridad Encapsulada.
- Función de dispersión para integridad y autenticación (MD5 o SHA).
- Algoritmo de cifrado (3DES, 40-bit DES y DES-CBC).

Llegan a un acuerdo sobre lo que se va a usar y se establecen dos asociaciones de seguridad, una para cada sentido.

b) Refresco de las claves de sesión.
Se refrescan las claves si es necesario.

c) La asociación de seguridad y las claves se pasa al driver IPSec junto con el SPI.

Todo lo acontecido en esta fase se encripta usando la ISAKMP Asociación de Seguridad negociada en la primera fase. Se encripta toda la carga útil de los paquetes ISAKMP excepto su cabecera.

Para concluir, podemos decir que seguridad con el protocolo de Internet provee de una buena seguridad en el nivel de red para IP, su protocolo establecido ISAKMP/Oakley, es un protocolo de seguridad que protege contra los ataques de posibles intrusos en la red durante se este conectado un usuario.

III.5 APLICACIONES

Para utilizar seguridad con el protocolo de Internet en una red, es preciso que todos los equipos y usuarios sean entidades conocidas y verificables. Seguridad con el protocolo de Internet proporciona un mayor grado de tranquilidad a los administradores, ya que impide la realización de muchas prácticas indebidas en la red. La principal aplicación de seguridad con el protocolo de Internet es en redes privadas virtuales (VPN

– Virtual Private Network), proveyendo así protección para los protocolos clientes que residen sobre la capa IP.

Una Red Privada Virtual (VPN - Virtual Private Network) no es sino una solución que nos permite disfrutar de un servicio de conectividad segura y fiable sobre una red pública, un medio compartido. En función de las características de este medio, o más exactamente de los protocolos empleados y tipo de red, se pueden distinguir diferentes tipos de redes privadas virtuales.

En una red IP, si no se restringe por otros medios, dos usuarios conectados pueden tener visibilidad mutua. Esta posibilidad, donde precisamente radica el éxito de Internet, debe administrarse con prudencia cuando hablamos de el protocolo de Internet de redes privadas virtuales, ya que dentro del marco de las mismas, sólo deberán poder acceder a los recursos del protocolo de Internet de redes privadas virtuales los usuarios habilitados para ello.

Seguridad con el protocolo de Internet proporciona la capacidad de hacer segura las comunicaciones a través de una red de área local (LAN – Local Area Network), una red de área extensa (WAN – Wide Area Network) privada o pública y a través de Internet. Algunos ejemplos de su uso o aplicaciones son los siguientes:

- Conectividad segura entre oficinas sucursales a través de Internet: una compañía puede construir una red privada virtual sobre Internet o a través de una red WAN pública. Esto permite a un negocio apoyarse firmemente en Internet y reducir su necesidad de una red privada, ahorrando costes y gestión de red suplementaria.

- Acceso remoto seguro a través de Internet: un usuario final cuyo sistema está equipado con protocolos de seguridad IP puede hacer llamadas locales a su proveedor de servicios Internet (PSI) y acceder de forma segura a una red de una compañía. Esto reduce el costo de los gastos de peaje de los empleados de viaje y de los abonados.

- Establecimiento de conectividad Intranet y Extranet con asociados: seguridad con el protocolo de Internet se puede utilizar para hacer las comunicaciones seguras con otras organizaciones, asegurando la autentificación y la privacidad y proporcionando un mecanismo de intercambio de claves.

- Mejorando la seguridad en el comercio electrónico: incluso aunque algunas aplicaciones web y de comercio electrónico tienen protocolos de seguridad internos, la utilización de seguridad con el protocolo de Internet mejora tal seguridad.

La principal característica de seguridad con el protocolo de Internet que le permite soportar estas aplicaciones variadas es que puede cifrar y/o autentificar el tráfico a nivel IP. Todas las aplicaciones distribuidas, incluyendo la conexión remota, cliente/servidor, correo electrónico, transferencia de ficheros, acceso a la red Internet y muchas más, se pueden hacer seguras.

III.6 ÁMBITO

Seguridad con el protocolo de Internet proporciona tres facilidades principales:

1. Una función de sólo autentificación conocida como cabecera de autentificación (AH,- Authentication Header).
2. Una función combinada de autentificación/cifrado llamada carga útil de seguridad encapsulada (ESP,- Encapsulating Security Payload).
3. Y una función de intercambio de claves.

De un modo lógico, seguridad con el protocolo de Internet funciona en cualquiera de estos tres modos:

- Anfitrión a Anfitrión
- Anfitrión a Red
- Red a Red

En cualquier escenario en el que haya una red, el concepto de enrutador está implícito, como en anfitrión a enrutador (y este enrutador controla y cifra el tráfico para una red particular).

El protocolo de Internet IPv4, no provee por sí mismo de ninguna protección a las transferencias de datos. Ni siquiera puede garantizar que el remitente sea quien dice ser. Seguridad con el protocolo de Internet intenta remediarlo. Estos servicios vienen tratados como dos servicios distintos, pero seguridad con el protocolo de Internet ofrece soporte para ambos de un modo uniforme

La forma en la que se configuran los sistemas de seguridad con el protocolo de Internet y las pasarelas es, hasta un cierto punto, trabajo del diseñador; sin embargo, el RFC contiene algunas recomendaciones importantes sobre cómo se debería implementar para evitar al máximo la confusión. Existen dos entidades administrativas que controlan lo que le ocurre a un paquete. Una es la base de datos de la asociación de seguridad (SAD - Security Association Database), y el otro es la base de datos de la política de seguridad (SPD - Security Policy Database).

Las dos se parecen en que, dado un número de selectores que describan algo de tráfico, entregarán una entrada que describa el proceso necesario. Sin embargo, SPD se elimina a dos pasos del proceso: SPD se usa para paquetes salientes, para decidir qué entradas SAD se deben usar, y qué entradas SAD describen el proceso y sus parámetros. Las entradas SPD especifican las entradas SAD existentes a usar, pero si no hay una que se pueda usar, entonces se usa para crear otras nuevas. Los campos de la asociación de seguridad que se crean se pueden tomar de la entrada SPD o del paquete que inició la creación.

Los paquetes salientes van desde la entrada SPD a la especificada de la asociación de seguridad, para obtener parámetros de codificación. Los paquetes entrantes obtienen la asociación de seguridad correcta directamente, y de ahí van a la entrada SPD.

La base de datos de la política de seguridad (SPD - Security Policy Database) también puede especificar qué tráfico debería circunvalar IPsec, y cuál se debería dejar caer, así que también debe ser consultado para tráfico no IPsec entrante. Las entradas de la base de datos de la política de seguridad se deben ordenar de forma explícita, ya que varias podrían coincidir con un paquete particular, y el proceso debe ser reproducible.

Se puede pensar en la base de datos de la política de seguridad como algo parecido a un filtro de paquetes, en el que las acciones que se deciden son la activación de procesos de una asociación de seguridad. Los selectores pueden incluir direcciones de origen y destino, números de puertos si fueran relevantes, nombres de anfitriones, niveles de sensibilidad de seguridad, protocolos, etc.

Una entrada de base de datos de la asociación de seguridad (SAD – Security Association Database) incluye:

- Dirección IP de destino.
- Protocolo IPsec (AH o ESP).
- Un índice de parámetros de seguridad (SPI – Security Parameters Index).
- Contador de secuencias.
- Indicador de secuencia O/F.
- Ventana de información anti-réplica.
- Tipo AH e información.
- Tipo ESP e información.

- Información sobre el tiempo de vida.
- Indicadores de modos túnel/transporte.
- Información sobre el camino de unidad de transferencia máxima (MTU – Maxim Transfer Unit).

Una entrada de base de datos de la política de seguridad (SPD – Security Policy Database) contiene:

- Puntero a asociaciones de seguridad activas.
- Campos de selector.

Para redes privadas virtuales generalmente se desean autentificación y cifrado, ya que es importante asegurar que usuarios no autorizados no entren en la red privada virtual y asegurar que si hay personas dedicadas a hacer escuchas en Internet no puedan leer los mensajes enviados por la red privada virtual. Ya que ambas características son deseables, la mayoría de las implementaciones utilizan carga útil de seguridad encapsulada en lugar de cabecera de autenticación. La función de intercambio de claves permite el intercambio manual de claves así como un esquema automático. Las especificaciones de seguridad con el protocolo de Internet son bastantes complejas y se tratan en muchos documentos. Los más importantes de dichos documentos, publicados en noviembre de 1998, son los RFC's 2401, 2402, 2406 y 2408.

III.7 CABECERA DE AUTENTIFICACIÓN

La cabecera de autentificación proporciona un medio para la integridad de los datos y la autentificación de los paquetes IP. La característica de integridad de los datos asegura que la modificación no detectada del contenido del paquete no es posible en su

camino. La característica de autentificación habilita a un sistema final, o a un dispositivo de red le permite autentificar el usuario o la aplicación y filtrar el tráfico adecuadamente; así también, previene el ataque de suplantación de dirección observado actualmente en Internet. La cabecera de autentificación se basa en el uso de un código de autentificación de mensaje (MAC - Message Authentication Code); por lo tanto, las dos partes, emisor y receptor, deben compartir una clave secreta.

La autenticación o autentificación de mensajes se realiza mediante una sencilla manipulación criptográfica:

Se envía un mensaje en claro y se le acompaña con su versión cifrada condensada, denominada código de autentificación de mensaje. En recepción se vuelve a cifrar el mensaje con la misma clave, y se calcula de nuevo el código de autentificación de mensaje comprobando que coincide con el recibido junto con el mensaje.

Un código de autentificación de mensaje se genera tomando el último segmento de una versión cifrada del mensaje original en la que el tipo de cifrado haga que todos los bits cifrados sean función de todos los bits procedentes del mensaje claro.

Código de autentificación de mensaje es utilizado por una clave secreta para proporcionar autenticación e integridad, sin embargo, puede ser también utilizado en un modo bi-direccional; es decir, de un modo donde sólo conocen la clave el emisor y el receptor quienes pueden verificar el mensaje o autentificar un archivo. Como consecuencia, el hecho de que se tenga una clave proporciona protección a posibles virus. Un virus puede infectar un archivo y generar un nuevo código alterado, pero si el virus o el intruso no puede saber o conocer la clave, no puede generar un nuevo código de autentificación de mensaje, por lo tanto, el emisor de un mensaje puede saber que el mensaje ha sido alterado. La desventaja de el código de autentificación de mensaje es que es más lento que los algoritmos de las firmas digitales.

La autenticación de mensajes proporciona las siguientes ventajas y desventajas:

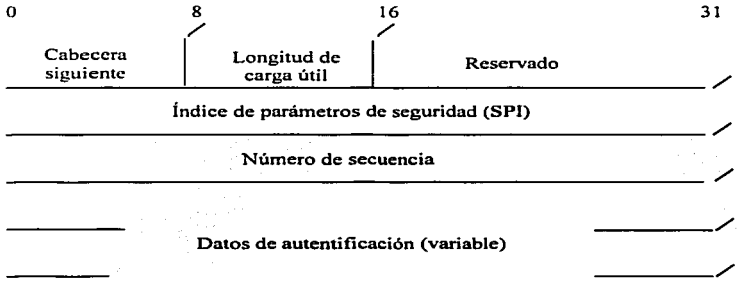
Ventajas:

- Asegura la integridad del mensaje.
- Mensajes iguales con clave igual, producen en diferentes momentos diferentes MAC según el estado inicial del registro de desplazamiento.
- Los mensajes utilizados parcialmente son rechazados, y se pueden detectar los mensajes reutilizados totalmente si se incluye una cabecera de mensaje con número de orden, hora y fecha.

Desventajas:

- No asegura su confidencialidad.
- Cualquier mensaje perturbado por el ruido de transmisión o por manipulación intencionada es rechazado por no auténtico.

La figura III.4 muestra la cabecera de autentificación con sus campos:



Figúra III.4 Cabecera de autentificación.

La cabecera de autenticación proporciona un medio para garantizar la integridad de los datos y la autenticación de los paquetes IP. La cabecera de autenticación consta de los siguientes campos:

- Cabecera siguiente (8 bits): identifica la cabecera que viene a continuación de ésta.
- Longitud de carga útil (8 bits): longitud del campo de datos de autenticación en palabras de 32 bits.
- Reservado (16 bits): para usos futuros.
- Índice de parámetros de seguridad SPI – Security Parameters Index (32 bits): identifica a una asociación de seguridad.
- Datos de autenticación (variable): número entero de palabras de 32 bits con los datos de autenticación

El contenido del campo de datos de autenticación dependerá del algoritmo usado al efecto. En cualquier caso, los datos de autenticación se calculan utilizando el paquete IP entero, poniendo a cero todos aquellos campos susceptibles de cambio en el tránsito.

CAPÍTULO IV
SEGURIDAD CON ENCRIPTAMIENTO

El proceso de codificar y descifrar mensajes se le llama encriptamiento y decriptamiento respectivamente. Criptografía es la ciencia y el arte de encriptar; se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial. El criptoanálisis, por su parte, es la ciencia y el arte de decriptar, se ocupa de romper los procedimientos de cifrado para así poder recuperar la información original. Frecuentemente, criptografía se utiliza para definir ambas palabras, encriptamiento y decriptamiento. Ambas disciplinas, criptografía y criptoanálisis, siempre se han desarrollado de forma paralela, ya que cualquier método de cifrado conlleva siempre su criptoanálisis correspondiente.

El encriptamiento como medio de proteger la información personal es un arte tan antiguo como la propia escritura. Como tal, permaneció vinculada durante mucho tiempo a los círculos militares y diplomáticos, ya que eran los únicos que en un principio tenían auténtica necesidad de ella. En la actualidad, la situación ha cambiado, el desarrollo de las comunicaciones electrónicas, unido al uso masivo y generalizado de los computadores, hace posible la transmisión y almacenamiento de grandes flujos de información confidencial que es necesario proteger. Es cuando el encriptamiento pasa a ser una exigencia de minorías a convertirse en una necesidad real del hombre, que ve en esta falta de protección de sus datos privados una amenaza para su propia intimidad.

La criptografía se utiliza para prever a cualquier mensaje de ser leído o alterado por un tercer usuario no autorizado, también llamado un intruso de la red Internet. El intruso puede ser pasivo, alguien que sólo esta escuchando o leyendo la información; o el intruso puede ser activo, cambiando el mensaje o la información o utilizar parte de dicha información sin el conocimiento ni la aprobación del emisor o del receptor originales. Es así, como el intruso puede identificarse como el emisor o el receptor del

mensaje original. Los usuarios que sólo escuchan o leen los mensajes sin alterarlos, reciben todo el mensaje completo y codificado pero no interfieren con la transmisión.

Un intruso activo interrumpe el mensaje que se envía desde el emisor hasta el receptor convirtiéndose en ambos, el receptor del mensaje original y el emisor. Este tipo de intrusos, también llamados estafadores (spoofers), tienen la habilidad de cambiar un mensaje militar y causar confusión en las tropas; o también, pueden utilizar la tarjeta de crédito de los usuarios de la red Internet y realizar compras muy caras. El emisor del mensaje debe asumir que sus datos pueden ser interceptados o alterados. Usuarios normales de correo electrónico pueden intercambiar mensajes a través del Internet sin ser del todo alterados, pero transferencias monetarias entre los bancos necesitan el método más seguro posible de encriptamiento.

Aún cuando se ha autenticado alguna información, ésta sigue siendo totalmente visible; el intruso puede intervenir las líneas de comunicación y estar recolectando toda la información que se envía. Para prevenir que esta información pueda serle de utilidad podemos encriptar los datos antes de enviarlos. El encriptamiento es necesario cuando necesitamos que la información que estamos enviando permanezca en secreto.

Los métodos de encriptamiento se puede clasificar en:

- Encriptamiento simétrico: es aquel en el que la clave de cifrado coincide con la de descifrado, dicha clave tiene que permanecer secreta, por lo que el emisor y el receptor se ponen de acuerdo previamente en la determinación de la misma.

- Encriptamiento asimétrico: es aquel en el que la clave de cifrado es diferente a la de descifrado, esta última conocida únicamente por el usuario.

Los métodos de encriptamiento simétricos son propios de la criptografía clásica o criptografía de clave secreta o privada, mientras que los métodos de encriptamiento asimétricos corresponden a la criptografía de clave pública. Antes, los procedimientos

de cifrado tenían una seguridad probable; hoy en día, los procedimientos de cifrado deben tener una seguridad matemáticamente demostrable. Esto lleva a una clasificación de seguridad criptográfica:

- Seguridad incondicional (teórica): el sistema es seguro frente a un atacante con tiempo y recursos computacionales ilimitados.
- Seguridad computacional (práctica): el sistema es seguro frente a un atacante con tiempo y recursos computacionales limitados; ejemplo: sistemas de clave pública basados en problemas de alta complejidad de cálculo.
- Seguridad probable: no se puede demostrar su integridad, pero el sistema no ha sido violado.
- Seguridad condicional: el sistema es seguro en tanto que el intruso del Internet de medios para atacar el sistema.

La figura IV.1 nos muestra la transmisión con datos encriptados.

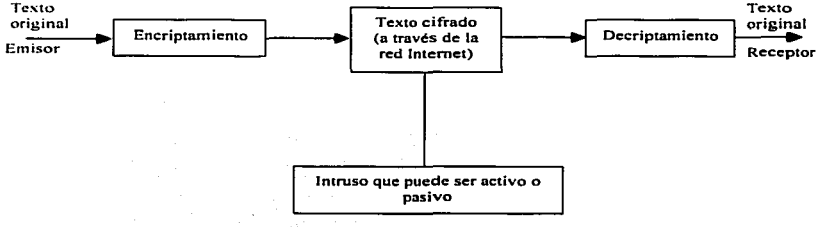


Figura IV.1 Transmisión de datos encriptados.

IV.1 TRANSMISIÓN SEGURA DE MENSAJES

Tres aspectos de mayor interés en el envío de datos privados o seguros a través de la red Internet son los siguientes:

- Los datos vienen de la persona que es identificada como el emisor.
- Los datos no son modificados.
- Los datos sólo son leídos por la persona a quien se le han enviado.

Para que el encriptamiento funcione adecuadamente, el emisor y el receptor tienen que conocer el conjunto de reglas llamado código que se utiliza para transformar la información original a su forma codificada, texto codificado. Un código simple podría consistir en agregar un número arbitrario de números, por ejemplo 13, a todos los caracteres en un mensaje; siempre y cuando la parte receptora conozca qué hizo el emisor al mensaje, la parte receptora puede invertir el proceso; por ejemplo, restar 13 caracteres a cada carácter en el mensaje recibido, para obtener el texto original. Un código es un conjunto de reglas para codificar datos.

El encriptamiento se basa en dos componentes: un algoritmo y una clave. Un algoritmo criptográfico es una función matemática que combina texto simple u otra información inteligible con una cadena de dígitos, llamada clave, para producir texto codificado ininteligible. La clave y el algoritmo usados son crucial para el encriptamiento.

Aunque sí existen algunos algoritmos de encriptamiento especiales que no usan una clave, los algoritmos que usan claves son particularmente importantes. Apoyar el encriptamiento en un sistema basado en clave ofrece dos ventajas importantes; la primera, los algoritmos de encriptamiento son difíciles de diseñar, uno como usuario no nos gustaría emplear un nuevo algoritmo cada vez que se comunique de manera privada con un nuevo receptor; al emplear una clave, se puede usar el mismo algoritmo

para comunicarse con muchas personas, todo lo que se tiene que hacer es usar una clave diferente con cada receptor. La segunda ventaja es, si alguien puede descifrar los mensajes encriptados, sólo tendrá que cambiar a una nueva clave para volver a encriptar mensajes, sin necesidad de cambiar a un nuevo algoritmo, a menos que el algoritmo, y no la clave, se sospeche sea inseguro, cosa que puede suceder, aunque es poco probable.

El número de posibles claves que cada algoritmo puede soportar depende del número de bits en la clave. Por ejemplo, una clave de 8 bits sólo permite 256 posibles combinaciones numéricas. Entre mayor sea el número de posibles claves, más difícil será descifrar un mensaje encriptado. El nivel de dificultad depende, por lo tanto, de la longitud de la clave. Una computadora no necesita mucho tiempo para probar secuencialmente cada una de las 256 claves posibles (menos de un milisegundo) y desencriptar el mensaje para ver si éste cobra sentido. Sin embargo, si se usara una clave de 100 bits (que equivale a examinar 2100 claves), una computadora que pruebe un millón de claves cada segundo podría tardar muchos siglos en descubrir la clave correcta.

La forma más antigua de criptografía basada en clave se denomina clave secreta o encriptamiento simétrico. En este tipo de transmisión, de encriptamiento simétrico, el emisor y el receptor poseen la misma clave, lo que significa que ambas partes pueden encriptar y desencriptar datos con la clave, como se muestra en la figura IV.2.

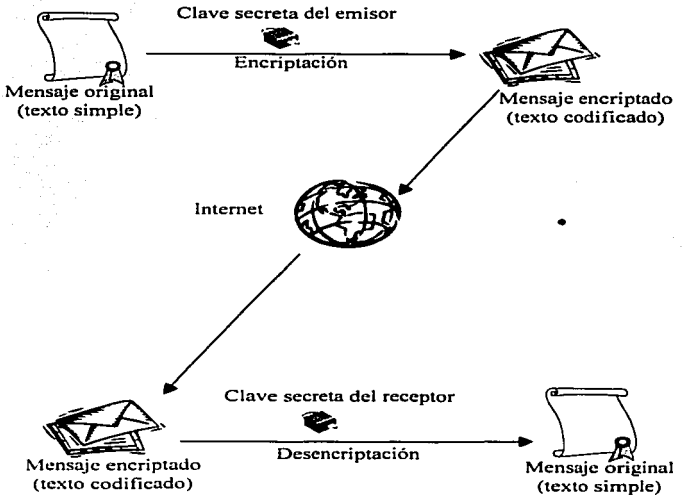


Figura IV.2 El encriptamiento simétrico usa una sola clave secreta para encriptar y desencriptar mensajes.

El encriptamiento simétrico presenta algunas desventajas, por ejemplo, ambas partes deben ponerse de acuerdo en usar una clave secreta compartida. Si en alguna empresa, o compañía, o negocio se tiene n receptores, entonces se debe dar seguimiento a n claves secretas, una para cada uno de sus receptores. Si se utiliza la misma clave para más de un receptor, significa que dichos receptores podrán leer entre si sus respectivos mensajes.

Métodos simples para disfrazar o cubrir mensajes no son muy apropiados para la transmisión segura de mensajes a través de la red Internet. Un ejemplo simple del método de descifrar claves es el de sustituir una letra por otra. Este método tan simple lo podemos encontrar o llevar a cabo en las revistas de acertijos o de formar y encontrar palabras. Sin embargo, dicho problema es fácilmente resuelto por programas de computadora que lleva a cabo varias posibles combinaciones de palabras y después proyecta la palabra más acertada. Las personas que se dedican a resolver acertijos no llevan a cabo todas las posibles combinaciones de palabras. A pesar de eso, utilizan caracteres conocidos del lenguaje para poder tener acceso al código real.

Un método efectivo de encriptamiento debe ocultar el número de caracteres en cada palabra, la existencia de doble letras, el lugar donde las vocales están, etc. Transmisión segura a través de la red Internet requiere de técnicas más complejas ya que hay muchas personas que pueden tener acceso a datos a través de la red y posiblemente alterar los mensajes, sin que los demás usuarios se den cuenta de que sus mensajes son leídos por otras personas.

IV.2 SERVICIOS DE SEGURIDAD

Los servicios de seguridad sólo pueden detectar abusos o cambios en el mensaje, pero no recuperarlos. Los mensajes vulnerables incluyen enmascaramiento, secuencia del mensaje, modificación de la información, negar algunos servicios, rechazar algunos mensajes, y que la información llegue a personas no deseadas. Cuatro de los servicios que caracterizan una buena seguridad en un sistema de red son:

- Integridad de los datos.- es la seguridad o afirmación de que los datos recibidos son los mismos que los datos que se enviaron.

- Autentificación.- es la verificación de la identidad del usuario quien genera el mensaje (datos) y la integridad de los datos. El usuario cuya identidad es verificada se le denomina como el principal, y el usuario quien demanda confirmación de la identidad del principal se le denomina verificador. Técnicas de autentificación difieren en varias maneras: deben asegurarse cuando el principal envía el mensaje o que este presente cuando el mensaje es enviado; deben apoyar a uno o a varios usuarios; o a veces deben permitir a un verificador comprobar a un tercer usuario que el mensaje fue enviado por el principal.

- Confidencialidad.- es la protección de la información de no ser revelada a aquellos que no deben recibirla. Este tipo de servicio es una opción en los métodos de autentificación. Encripta los mensajes utilizando algoritmos, ya sea de encriptamiento simétrico o asimétrico. El enviar mensajes a varios destinatarios requiere de técnicas simétricas, ya sea sólo esta técnica o la combinación con técnicas asimétricas.

- Autorización.- es el proceso en el que uno determina si al principal se le permite llevar a cabo alguna operación. El proceso usualmente sigue una autentificación y puede ser basado bajo la información disponible del verificador o por la autorización de otros usuarios.

A continuación se proporcionara el nombre de algunas empresas que ofrecen dichos servicios de seguridad en redes con su respectiva dirección de su sitio en la red Internet, donde se encontrara mayor información de dichas empresas:

VERISIGN (www.verisign.com).

Es una empresa que desde hace varios años ofrece el servicio de seguridad, tanto a empresas que requieran transacciones en línea, como certificados y encriptación de correo electrónico a los usuarios de Internet. Sus certificados de seguridad, que encriptan información e identifican al usuario, pueden ser descargados desde su

página, tienen un periodo de prueba de treinta días y después cada año tiene un costo de $5 dólares; soporta Eudora, Outlook de Microsoft y Messenger de Netscape.

NAI Associates (www.nai.com).

Es la alianza que incluye en sus filas a McAfee, tiene la particularidad de ser el concesionario de la tecnología de Muy Buena Privacidad (PGP - Pretty Good Privacy) y la vende a nivel internacional, enfocándose a las empresas que requieren de estos servicios comerciales. Cuentan con presencia en México y es posible adquirir este producto con un nivel de seguridad alto.

PGP (www.pgp.com).

Se dice que es la mejor en el arte del encriptamiento; con todo y que su autor por poco y enfrenta cargos criminales por distribuirlo a través de la red, es el producto más completo, poderoso y seguro que se pueda encontrar. Si alguien lo requiere para fines personales y no lucrativos, se puede obtener sin costo desde su página de Internet. Es toda una familia de productos que no sólo protegen los correos, también puede encriptar archivos, discos y conexiones de red, además de ofrecer autentificación de los usuarios de los recursos. Soporta Eudora, Outlook y otros, principalmente en las plataformas Win95/98/NT/2000, Solaris, MacOS y Linux. Su única limitante es que es destinado sólo a ciudadanos de E.E.U.U.

GPG (www.gnupg.com).

Es una nueva empresa que ofrece los servicios de seguridad, reemplazó a PGP en alguna medida como una solución mucho más accesible internacionalmente debido a su desarrollo fuera de los Estados Unidos. GPG está ganando popularidad, particularmente después de que NAI retiró el apoyo comercial a PGP, y el despegue de Linux.

Pepe.net (http://pepe.net.mx).

Es una empresa donde se han dedicado desde hace algún tiempo a vender versiones personalizadas de Linux, y lo interesante es que sus distribuciones incluyen Muy Buena Privacidad (PGP - Pretty Good Privacy) para servidor, además que ellos tienen sus propios certificados de autentificación que se activan en el momento que se accesa a su servidor, que cuenta con una conexión segura.

IV.3 ALGUNOS ALGORITMOS DE ENCRIPTAMIENTO SIMÉTRICO Y ASIMÉTRICO

Una fuente de información en cuanto a problemas de seguridad y herramientas para solucionar los problemas de seguridad es la consultoría llamada Equipo de Respuestas a Emergencias Informáticas (CERT - Computer Emergency Response Team). Dicha consultoría fue formada por la Agencia de Proyectos Avanzados de Investigación para la Defensa (DARPA - Defense Advanced Research Projects Agency) en 1988, manteniendo su centro de coordinación en el Instituto de Ingeniería en Software de la universidad Carnegie Mellon.

No importa que tan efectiva y bien administrada sea cualquier tipo de red, dicha red es vulnerable a ser atacada por intrusos que quieran algún tipo de información que no les corresponde. La gran variedad de redes vulnerables incluyen acceso a archivos con una clave secreta, correos electrónicos, acceso remoto, y directorio de escritura de Protocolo de Transferencia de Archivos (FTP - File Transfer Protocol), entre muchos más. Un gran número de herramientas están disponibles para apoyar al administrador de red en detectar ataques e implementar seguridad cuando sea necesario.

Algunos algoritmos de encriptamiento como lo es el estándar de encriptamiento de datos, Diffie-Hellman, etc., son muy comunes y viables, pero existen otros más que tienen la escena de agregar mayor seguridad en el Internet. Enseguida se nombrara y se dará una breve explicación, sin entrar a detalle, de los aspectos que se consideran más importantes de algunos de los algoritmos de encriptamiento de datos más utilizados, tanto simétricos como asimétricos.

Algoritmos de encriptamiento simétricos:

- Estándar de Encriptamiento de Datos (DES - Data Encryption Standard).

El estándar de encriptamiento de datos, es un codificador de bloque creado por IBM en 1973, avalado por el gobierno de los Estados Unidos en 1977. Usa una clave de 56 bits y opera en bloques de 64 bits. Relativamente rápido; se usa para encriptar grandes cantidades de datos al mismo tiempo. Posteriormente se sacó una versión de estándar de encriptamiento de datos implementada por hardware, que entró a formar parte de los estándares de la Organización Internacional para la Normalización (ISO - International Standard Organization) con el nombre de algoritmo de cifrado de datos (DEA - Data Encryption Algorithm). Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits, para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, el estándar de encriptamiento de datos utiliza una clave simétrica de 64 bits, de los cuales 56 bits son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso. Como la clave efectiva es de 56 bits, son posibles un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.

Las principales desventajas que presenta el estándar de encriptamiento de datos son:

- Se considera un secreto nacional de EEUU, por lo que está protegido por leyes específicas, y no se puede comercializar ni en hardware ni en software fuera de ese país sin permiso específico del departamento de estado.
- La clave es corta, tanto que no asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema. Pero con la potencia de cálculo actual y venidera de los computadores y con el trabajo en equipo por Internet se creé que se puede violar el algoritmo, como ya ha ocurrido una vez, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.
- No permite longitud de clave variable, con lo que sus posibilidades de configuración son muy limitadas, además de permitirse con ello la creación de limitaciones legales.
- La seguridad del sistema se ve reducida considerablemente si se conoce un número suficiente de textos elegidos, ya que existe un sistema matemático, llamado criptoanálisis diferencial, que puede en ese caso romper el sistema en 2 elevado a 47 iteraciones.

Entre sus ventajas cabe citar:

- Es el sistema más extendido del mundo, el que más máquinas usan, el más barato y el más probado.
- Es rápido y fácil de implementar.
- Desde su aparición nunca ha sido roto con un sistema práctico.
- Ofrece un alto nivel de protección de datos contra personas no autorizadas y modificaciones de datos no autorizados.
- Simple de entender.

- Protección en método de ecriptamiento en lugar de basarse en un algoritmo secreto.
- Eficiente para operar.
- Adaptable para diferentes aplicaciones.
- Disponible para todos los usuarios a un costo razonable.

Actualmente el estándar de encriptamiento de datos ya no es estándar y fue roto en Enero de 1999 con un poder de cómputo que efectuaba aproximadamente 250 mil millones de ensayos en un segundo.

- Triple Estándar de Encriptamiento de Datos (3-DES - Triple Data Encryption Standard).

Basado en el estándar de encriptamiento de datos, el triple estándar de encriptamiento de datos encripta un bloque de datos tres veces, con tres claves diferentes. Se ha propuesto como una alternativa al estándar de encriptamiento de datos y su uso se incrementa día con día, pues se ha hablado mucho acerca de la posibilidad de violar el estándar de encriptamiento de datos con facilidad y rapidez. Este sistema de encriptamiento es una variante del estándar de encriptamiento de datos. La diferencia entre el estándar de encriptamiento de datos (DES) y el triple estándar de encriptamiento de datos (3-DES) radica en que el último algoritmo realiza dos operaciones de encriptamiento y una de decriptamiento usando el algoritmo de estándar de encriptamiento de datos. La principal desventaja del triple estándar de encriptamiento de datos es que es tres veces más lento. El inconveniente de la velocidad se hizo en pro de conseguir mayor seguridad, ya que a diferencia de su antecesor, el triple estándar de encriptamiento de datos si es seguro. Para evitar ataques de fuerza bruta con este algoritmo es necesario usar dos claves de 56 bits cada una. El uso de dos claves produce inconvenientes pues hace más tedioso el manejo de las mismas.

Otra desventaja que tiene el triple estándar de encriptamiento de datos, es que el diseño de las Cajas-S (cadena de bits o números binarios que pueden representarse por los valores en hexadecimal) es puesto en duda por una parte considerable de la comunidad de criptoanalistas.

El sistema del estándar de encriptamiento de datos se considera en la actualidad poco práctico, debido a la corta longitud de su clave. Para solventar este problema se creó el sistema triple estándar de encriptamiento de datos, basado en tres iteraciones sucesivas del algoritmo estándar de encriptamiento de datos, con lo que se consigue una longitud de clave de 128 bits y se divide en dos diferentes de 64 bits, y que es compatible con el estándar de encriptamiento de datos simple.

- Algoritmo Internacional de Encriptamiento de Datos (IDEA - International Data Encryption Algorithm).

El algoritmo internacional de encriptamiento de datos fue creado en 1991 y diseñado para ser eficaz. Ofrece un encriptamiento muy poderoso, ya que los datos están compuestos por bloques de 64 bits, mientras que la clave consta de 128 bits. El algoritmo internacional de encriptamiento de datos es un sistema de encriptamiento que en su diseño tomó en cuenta el hecho que existen nuevas técnicas de criptoanálisis tales como el criptoanálisis diferencial. Gracias a este hecho el algoritmo usado por el algoritmo internacional de encriptamiento de datos es considerado bastante seguro contra este tipo de ataques. Hasta ahora no ha habido ningún ataque que haya podido penetrar la seguridad de este algoritmo, sin embargo, es conveniente mencionar que para que un sistema de encriptamiento pueda ser considerado confiable es recomendable que supere dos décadas de vida pública sin que haya podido romperse su seguridad. El principal inconveniente que presenta el algoritmo internacional de encriptamiento de datos es su corta vida, pues fue creado a principios de la década de los noventa por lo que todavía carece del tiempo recomendable para poderlo considerar seguro.

Se estima que al implementar el algoritmo internacional de encriptamiento de datos en hardware se puede obtener un rendimiento de 177 Mbps. A pesar de las altas velocidades que se pueden lograr a través de chips dedicados, se estima que una implementación en software de este sistema de encriptamiento podría presentar un rendimiento de alrededor de 200 Kbps. Este bajo rendimiento en software hace impráctica la implantación del algoritmo internacional de encriptamiento de datos en dispositivos de bajo poder computacional tales como celulares. El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta, con la salvedad de que los sub-bloques de clave de desencriptado son distintos, calculándose como los inversos de los sub-bloques de encriptado y también en orden inverso. El método de expansión de clave se inicia dividiendo la palabra clave de 128 bits, introducida por el usuario, en ocho subclaves de 16 bits, que constituyen los ocho primeros sub-bloques de clave; posteriormente se rota la clave 25 bits hacia la izquierda y se obtienen los siguientes ocho sub-bloques de clave, y así sucesivamente.

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como muy buena privacidad (PGP – Pretty Good Privacy).

Algoritmos de encriptamiento asimétricos:

- DIFFIE-HELLMAN.

Existe una manera o un método para que dos personas, sin preparación previa, puedan establecer una clave de sesión secreta a través de una habitación o lugar público, repleto de gente, mediante el intercambio de mensajes visibles para todo el mundo, dicho método fue descubierto por Whitfield Diffie y Martin Hellman en la universidad de Stanford y publicado en 1976. Éste método es el sistema de encriptamiento de clave pública más antiguo todavía en uso. No soporta el

encriptamiento ni las firmas digitales. El sistema está diseñado para permitir que dos individuos se pongan de acuerdo en una clave compartida, aunque sólo intercambian mensajes en público. Su principal ventaja con respecto a sistemas de cifrado como el de clave pública con clave variable es que no necesita encriptar ni decriptar ninguna información que debe ser transmitida. Gracias a este hecho la velocidad con la que se puede establecer una clave con el protocolo Diffie-Hellman es mucho mayor. Sin embargo, la especificación de la función hecha por este protocolo es lo que lo hace impráctico para su uso en dispositivos portátiles, ya que además de la implementación del protocolo se requiere la implementación de los algoritmos simétricos que se usarán durante la comunicación.

El sistema de encriptamiento Diffie-Hellman opera de la siguiente manera: en primer lugar, se eligen un número primo grande P y un número r pequeño que es raíz primitiva de P (esto significa que los números r^1, r^2, r^3, ..., r^{P-1} son todos módulos de P diferentes). Los números P y r son completamente públicos. Posteriormente, Alicia elige un número secreto A, y Roberto selecciona un número secreto B, ambos comprendidos en el rango de 1 a P-1. Alicia mantiene secreto A pero calcula el número $\alpha = r^A$ módulo P y lo apunta y lo muestra. De manera análoga, Roberto mantiene confidencial B, pero calcula $\beta = r^B$ módulo P, lo apunto y lo exhibe para que todos lo vean. Alicia ahora calcula β^A módulo P, y Roberto determina α^B módulo P, ambos son el mismo número, r^{AB} módulo P. Este es su secreto compartido.

Diffie-Hellman funciona ya que matemáticamente es muy difícil obtener A si sólo se conoce P, r y r^A, cuando P es un número suficientemente grande. Habitualmente, la longitud del número P es como mínimo de 500 bits con el objeto de que el algoritmo sea computacionalmente invulnerable.

Existe la incertidumbre de que nadie es capaz de espiar la conversación que se está manteniendo con otra persona ya que se dispone de un secreto compartido fuertemente protegido, aunque con el sistema de encriptamiento Diffie-Hellman no se puede estar seguro de quien es la persona con quien se está hablando, pudiendo haber un impostor o intruso, retransmitiendo la información enviada entre dos personas, y tiene la oportunidad de registrar todo lo que se ha escrito o enviado e incluso la

oportunidad de introducir mensajes falsos. Por esta razón, Diffie-Hellman se emplea generalmente junto con algún tipo de técnica de identificación para asegurar que la otra persona con la que se está intercambiando información secreta es realmente la que se piensa que es.

- Skipjack - Clipper

A principios de 1994, el Instituto Nacional de Estándares y Tecnología (NIST – National Institute of Standards and Technology) aprobó el Documento de Estándar de Encriptamiento (EES – Escrowed Encryption Standard). El estándar consiste en un algoritmo clasificado llamado Skipjack; un chip de encriptamiento llamado Clipper; y claves secretas de encriptamiento todavía sin publicarse por el gobierno estadounidense. El documento de estándar de encriptamiento es un sistema voluntario y su intención es proporcionar encriptamiento de voz, fax, y transmisiones por computadora a través de los circuitos y sistemas telefónicos. El algoritmo de encriptamiento/decriptamiento de Skipjack se basa en técnicas de clave pública. Ya que emplea una clave de 80 bits, el método es considerado millones de veces más poderoso que el método del estándar de encriptamiento de datos con clave de 56 bits. El chip de la parte de Clipper contiene una clave adicional. El equipo es manufacturado, el chip es instalado y la clave se divide en dos partes, cada mitad es puesta en custodia por una institución.

Es tecnológicamente posible colocar un chip en dispositivos para que los mensajes a través de dicho dispositivo puedan ser monitoreados. La factibilidad o posibilidad de Skipjack - Clipper, no es un resultado tecnológico. Sin embargo, el documento de estándar de encriptamiento levanta controversias políticas y sociales, especialmente en crear un derecho individual a la privacidad contra el sistema del gobierno para proteger a sus ciudadanos.

El chip de cifrado Clipper fue diseñado para equilibrar los intereses contrapuestos de las agencias gubernamentales con los de los ciudadanos y la industria privada. Las agencias gubernamentales desean tener acceso a las comunicaciones de criminales sospechosos; por ejemplo interceptar sus líneas telefónicas. La industria privada y los ciudadanos desean coreo electrónico y comunicaciones seguras, y ven la criptografía como el medio de proporcionárselas. La tecnología Clipper, intenta atender ambas necesidades utilizando claves bajo custodia. El chip Clipper ha sido propuesto como estándar gubernamental de los E.E.U.U.; debería entonces ser utilizado por cualquiera que tenga negocios con el gobierno federal, así como para las comunicaciones dentro del propio gobierno, sin embargo, la utilización de Clipper es totalmente voluntaria.

El chip Clipper contiene un algoritmo de cifrado denominado Skipjack, el chip contiene una clave unitaria de 80 bits, que es custodiada en dos partes y en dos agencias de custodia diferentes; se deben conocer ambas partes si se desea recuperar la clave. También está presente un número de serie y una clave conocida de 80 bits. El chip está fabricado de forma que no es posible realizar una ingeniería inversa, es decir, que el algoritmo Skipjack y sus claves no se pueden extraer del chip.

Skipjack es el algoritmo de cifrado contenido en el chip Clipper y fue diseñado por la Agencia de Seguridad Nacional (NSA - National Security Agency). Utiliza una clave de 80 bits para cifrar bloques de datos de 64 bits y que es la misma clave utilizada para descifrar. Se puede utilizar Skipjack de la misma forma que el estándar de encriptamiento de datos, y quizás más segura, ya que transforma los datos en 32 pasos o bloques. El algoritmo Skipjack no puede ser implementado por software, sino por el hardware de fabricantes de chips autorizados por el gobierno.

IV.4 SISTEMAS DE ENCRIPTAMIENTO DE CLAVE PRIVADA Y PÚBLICA

Dos tipos de criptografía, simétrica y asimétrica, pertenecen respectivamente, a los métodos de encriptamiento y decriptamiento siendo utilizados por los emisores y receptores, ya sea privada o públicamente. En los sistemas de criptografía simétrica, los métodos de encriptamiento y decriptamiento son compartidos privadamente por los emisores y receptores. La criptografía asimétrica utiliza métodos públicos que son certificados por autoridades, y el método de encriptamiento es cambiado por una clave pública, permitiendo al receptor decodificar el texto cifrado. Dichas autoridades, son un mecanismo para asegurar que las claves y los métodos y las identidades de los usuarios, los cuales todos son públicos, sean correctos.

La criptografía de clave pública se basa en el concepto de un par de claves. Cada mitad del par (una clave) puede encriptar información que sólo la otra parte (la otra clave) podrá desencriptar. Una parte del par de claves, la clave privada, sólo es conocida para el propietario designado; la otra parte, la clave pública, se publica abiertamente, pero continúa asociada al propietario. Los pares de claves tienen una característica única: los datos encriptados con una clave sólo pueden desencriptarse con la otra clave del par. En otras palabras, no tiene importancia que el emisor use la clave privada o la clave pública para encriptar un mensaje, ya que el receptor puede usar la otra clave para desencriptarlo.

Las claves pública y privada se pueden usar de dos maneras diferentes: para proporcionar confidencialidad al mensaje y para probar la autenticidad del emisor de un mensaje. En el primer caso, el emisor usa la cave pública del receptor para encriptar un mensaje, de manera que el mensaje continúe siendo confidencial hasta que sea decodificado por el receptor con la clave privada. En el segundo caso, el emisor encripta un mensaje usando la clave privada, una clave a la cual sólo tiene acceso el emisor. La clave pública del receptor asegura la confidencialidad; la clave privada del emisor verifica la identidad del emisor.

Por ejemplo, para crear un mensaje confidencial, una persona necesitará conocer primero la clave pública de su receptor. Después, deberá usar la clave pública del receptor para encriptar el mensaje y enviarlo. Como el mensaje se encriptó con la clave pública del receptor, sólo alguien con su clave privada puede desencriptar el mensaje.

La regla general para elegir el mejor método de encriptamiento es la siguiente: primero se determina qué tan sensibles son los datos y por cuánto serán sensibles y necesitan estar protegidos, una vez que se sepa, se selecciona un algoritmo de encriptamiento y longitud de clave que tome más tiempo en descifrarse que el período de tiempo por el cual los datos serán vulnerables. Ningún sistema de encriptamiento es ideal para todas las situaciones, la tabla IV.1 ilustra algunas de las ventajas y desventajas de cada tipo de encriptamiento.

Encriptamiento	Ventajas	Desventajas
Clave privada.	Rápida.	Ambas claves son la misma.
	Se puede instrumentar fácilmente en hardware.	Dificultad para distribuir las claves.
		No soporta las firmas digitales.
Clave pública.	Usa dos claves diferentes.	Lenta y exhaustiva.
	Claves relativamente fáciles de distribuir	
	Proporciona integridad y no repudiamiento mediante firmas digitales.	

Tabla IV.1 Ventajas y desventajas de los sistemas criptográficos

La tabla IV.2 muestra las distintas longitudes existentes en bits para el encriptamiento de clave privada y clave pública.

Longitud de la clave privada	Longitud de la clave pública
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

Tabla IV.2 Longitudes de clave privada y clave pública para niveles equivalentes de seguridad

Cuando se trata de seleccionar el software o hardware para propósitos de seguridad, hay que mencionar que se puede usar más de un sistema de encriptamiento en el producto, ésta es una práctica común debido a los distintos requerimientos computacionales para los algoritmos de clave privada y clave pública.

IV.4.1 Encriptamiento de clave privada

El encriptamiento de clave privada se caracteriza por los métodos de codificación y decodificación conocidos sólo por los emisores y receptores autorizados. El más prominente de este tipo de métodos es el estándar de encriptamiento de datos (DES – Data Encryption Standar).

La aparente complejidad del estándar de encriptamiento de datos es engañosa, es demasiado rápida para ser efectiva, especialmente para mensajes con gran contenido de información. El estándar de encriptamiento de datos en su implementación original, no puede ser considerado un método seguro; una de las razones es que los mismos 64 bits del bloque del texto original o el mensaje original siempre produce los mismos 64 bits del bloque encriptado. Algunos métodos de encadenamiento pueden ser utilizados para aumentar la seguridad del método, aunque también incrementa su complejidad. El estándar de encriptamiento de datos también se utiliza en combinación con el encriptamiento de clave pública.

IV.4.2 Encriptamiento de clave pública

En el año de 1976, Whitfield Diffie y Martin Hellman propusierón un método diferente para transmitir mensajes encriptados a través de la red. El concepto, creo la clave pública de encriptamiento pero mantuvo la clave secreta de decriptamiento, trajo una alternativa viable para el estándar de encriptamiento de datos. Abrió las puertas para expandir el concepto o el papel de criptografía en sectores públicos y privados. Dicho método permite a los usuarios combinar los dos métodos, tomando ventaja de las mejores estructuras de ambos métodos.

El sistema de encriptamiento de clave pública requiere que cada usuario tenga una clave de codificación-decodificación. La clave de codificación E (Encoding key), se hace pública; la clave de decodificación D (Decoding key), es conocida sólo por el usuario. Un sistema efectivo de encriptamiento de clave pública debe tener los siguientes componentes:

- Las claves E y D deben ser la función inversa; es decir, si M es el mensaje, entonces tenemos D(E(M))=M. Esto significa que el mensaje enviado debe ser el mensaje recibido.
- La cantidad de sistemas computacionales para aplicar E y D deben ser razonables.

- E no puede ser roto sin conocer D; es decir, un mensaje encriptado no puede ser decriptado por ningún otro método que solo aplicar D.
- La cantidad de tiempo y esfuerzo para descubrir D debe ser complicado computacionalmente hablando.

Un método que combina encriptamiento de clave privada y encriptamiento de clave pública, sin las desventajas de ambos sistemas, es el de utilizar un sistema de clave pública con clave variable, también conocido como el método RSA, el cual se explico en el capítulo II.4. El emisor puede encriptar el mensaje con ayuda del estándar de encriptamiento de datos, el receptor decripta los mensajes que contienen claves de estándar de encriptamiento de datos aplicando la clave secreta D. Esta combinación de métodos provee la capacidad deseable de extender longitudes de claves para mantener los avances en técnicas de factorización.

La combinación de seguridad con encriptamiento de clave privada y clave pública se crea o nace a partir de proteger información contra los intrusos del Internet. Intrusos pasivos, intrusos activos, o que solamente monitorean el tráfico en la red, si no tienen la clave secreta decodificadora D no tienen acceso a las claves encriptadas del estándar de encriptamiento de datos con la clave pública codificada E. El intruso activo debe conocer todas las claves para poder decriptar y encriptar el mensaje, poderlo alterar, y después encriptar el mensaje ya alterado. Cuando las claves del estándar de encriptamiento de datos son encriptadas con una clave de codificación E, el intruso activo debe conocer la clave secreta D para decodificar y obtener las claves del estándar de encriptamiento de datos.

Aunque encriptar un mensaje con una clave pública no difiere mucho de usar un encriptamiento de clave secreta, los sistemas de clave pública presentan ciertas ventajas. Por ejemplo, la clave pública del par de claves se puede distribuir prontamente, en un servidor, sin temor de que esto comprometa el uso de la clave privada. Por ello, el usuario no tiene que enviar una copia de su clave pública a todos

sus receptores; ya que ellos la pueden obtener desde un servidor de clave mantenido por su compañía, o quizás a través de un proveedor de servicio.

Otra ventaja de la criptografía con clave pública es que permite que se autentifique al emisor del mensaje. La idea básica es la siguiente: ya que el usuario es la única persona que puede encriptar algo con su clave privada, todo aquel que use la clave pública del usuario emisor para desencriptar el mensaje puede estar seguro de que el mensaje proviene de quien lo envió. Así, el uso de la clave privada en un documento electrónico es similar a la firma en un documento de papel. Pero no hay que olvidar que aunque el receptor puede estar seguro de que el mensaje proviene del emisor original, no hay forma de garantizar que alguien más lo haya leído con anterioridad.

IV.5 SEGURIDAD EN CORREO ELECTRÓNICO

Desde que un mensaje de correo electrónico es enviado a través de Internet hasta que llega a su destinatario pasa por multitud de ordenadores servidores en los que puede ser leído o incluso manipulado. Hay que tener presente también lo fácil que resulta falsificar la dirección del remitente del mensaje.

Si lo comparamos con el correo ordinario, enviar un mensaje de correo electrónico sin encriptar equivaldría a enviar nuestra carta mecanografiada, sin firmar y en un sobre abierto. No es eso lo que hacemos habitualmente en nuestras comunicaciones postales.

Para obtener garantías suficientes de confidencialidad, autentificación e integridad en nuestro correo electrónico, y realizar algo similar a lo que hacemos con nuestro correo ordinario, firmando la carta y cerrando el sobre, podemos usar técnicas criptográficas.

Junto con la creciente popularidad del Internet se encuentra el crecimiento de la criptografía como un elemento para proporcionar autentificación, confidencialidad e integridad de los mensajes. A continuación se proporcionara una breve explicación acerca de algunos métodos de seguridad en correo electrónico, como lo son: Correo Privado Mejorado (PEM - Privacy Enhanced Mail) y Muy Buena Privacidad (PGP - Pretty Good Privacy).

Correo Privado Mejorado (PEM - Privacy Enhanced Mail)

El método de Correo Privado Mejorado es diseñado primeramente por usuarios de correo electrónico del Internet. Comenzó en 1985 por el Grupo de Investigación de Privacidad y Seguridad (PSRG – Privacy and Security Research Group) del Consejo de la Arquitectura de Internet (IAB – Internet Arquitecture Board) y desarrollado por la fundación de la Agencia de Proyectos Avanzados de Investigación (ARPA - Advance Research Projects Agency).

Correo Privado Mejorado es un estándar para correo electrónico seguro, definido en los RFC 1421 y 1424. Envuelve la esencia de los servicios de seguridad del modelo de Interconexión de Sistemas Abiertos (OSI - Open Systems Interconnect), que son: encriptamiento, autenticación y claves de certificación; además, define los algoritmos a ser utilizados.

Correo Privado Mejorado no genera autentificación en el receptor, siendo un estándar práctico, puede operar muy eficazmente en casi todos los sistemas de correo electrónico existentes.

Correo Privado Mejorado fue uno de los primeros estándares para asegurar los mensajes de texto del correo electrónico, fue definido por el Grupo de Ingeniería en Internet (IETF - Internet Engineering Task Force) como el método para encriptar mensajes de texto de 7 bits. Es también definido como una estructura jerárquica para distribuir y verificar las firmas digitales. Correo Privado Mejorado especifica una

infraestructura de clave pública para un intercambio de claves a través de grandes redes como el Internet.

Correo Privado Mejorado se trata de un borrador para una norma Internet que trata de dar seguridad a los servicios de correo electrónico. Se puede utilizar con el Protocolo de Transferencia de Correo Simple para Internet (SMTP – Simple Mail Transfer Protocol) o con cualquier otro esquema de mensajería, como X.400. Están contemplados servicios de autenticación y confidencialidad, así como la gestión de claves mediante certificados. Proporciona seguridad extremo a extremo, creando una cabecera encapsulada que se pone al principio del texto del mensaje.

Correo Privado Mejorado ha sido envuelto en un estándar virtual de Internet para el correo seguro, el cual, también se ha convertido en un producto comercial. Los pasos en el proceso de Correo Privado Mejorado es el de transformar el mensaje en una representación de estándar de la red, calculando el código de un mensaje integro, encriptando el mensaje, y transformando el mensaje final en un carácter óptimo para su transmisión. Correo Privado Mejorado permite una serie de algoritmos, incluyendo el estándar de encriptamiento de datos para encriptamiento y clave pública con clave variable para la autentificación del emisor y claves seguras.

El uso de Correo Privado Mejorado ha descendido, ya que no está diseñado para manejar el moderno correo electrónico de multipartes soportado por Extensiones Multipropósito del Correo en Internet (MIME - Multipurpose Internet Mail Extensions), además de que requiere una jerarquía rígida de autoridades de certificación para emitir claves.

Muy Buena Privacidad (PGP - Pretty Good Privacy).

P.R. Zimmerman desarrollo el método de Muy Buena Privacidad (PGP - Pretty Good Privacy) para una buena seguridad en correo electrónico y encriptamiento de archivos a través del Internet. El método apareció en 1991 como un producto gratis

disponible vía anónima en el Protocolo de Transferencia de Archivos (FTP - File Transfer Protocol) a través del Internet. Se comprobó que el método es efectivo y es utilizado por un gran número de ciudades como un estándar. Muy Buena Privacidad es un sistema de clave pública; internamente, es un híbrido del método del algoritmo internacional de encriptamiento de datos, una versión del estándar de encriptamiento de datos desarrollado por X. Lai y J. Massey en Suecia a principios de los 90's. Brevemente, los pasos básicos de encriptamiento/decriptamiento en el método de Muy Buena Privacidad son:

- Emisor: utiliza el algoritmo internacional de encriptamiento de datos para encriptar el mensaje con una clave generada al azar.
- Emisor: utiliza los recipientes de la clave pública para encriptar la clave generada al azar.
- Receptor: utiliza los recipientes de la clave privada para decriptar la clave del algoritmo de encriptamiento de datos.
- Receptor: utiliza la clave del algoritmo de encriptamiento de datos para decriptar el mensaje.

Muy Buena Privacidad probablemente sea la aplicación de seguridad para correo electrónico en Internet más usada; emplea una variedad de estándares de encriptamiento. Las aplicaciones para encriptamiento/desencriptamiento de Muy Buena Privacidad están disponibles de manera gratuita para la mayoría de los sistemas operativos importantes; así, los mensajes se pueden encriptar antes de usar un programa de correo electrónico. Muy Buena Privacidad se diseñó alrededor del concepto de una red de confianza que permitía a los usuarios compartir sus claves, sin requerir una jerarquía de autoridades de certificación.

Para usarlo hay que comenzar generando un par de claves, una pública y otra privada, siendo posible en ese momento la elección de la longitud de clave deseada. También hay que fijar una clave personal, que se usará luego para proteger la clave privada de posibles intrusos. Las claves pública y privada las genera automáticamente

el algoritmo, mientras que la personal de protección la elige el usuario. Una vez generadas las claves, la privada se encripta con la personal mediante un algoritmo simétrico, siendo posteriormente necesario desencriptarla cada vez que deseemos usarla.

En cuanto a la clave pública, se deposita en un fichero especial, de tipo código ASCII (sólo texto), denominado certificado de clave, que incluye el identificador de usuario del propietario (el nombre de esa persona y algún dato único, como su dirección de e-mail), un sello de hora del momento en el que se generó el par de claves y el material propio de la clave.

Normalmente el sistema Muy Buena Privacidad viene implementado mediante alguna aplicación específica, que se instala en el computador del usuario. Esta aplicación se integra perfectamente con los programas de correo más comunes, permitiendo al usuario el uso directo del sistema Muy Buena Privacidad, con tan sólo pulsar los botones que aparecerán en la barra de menús de la aplicación de correo.

Muy Buena Privacidad es uno de los sistemas de encriptamiento más utilizados para la seguridad en correo electrónico debido a las siguientes razones:

1. Es uno de los más difundidos y usados.
2. Es soportado por los sistemas operativos más habituales (DOS/Windows, UNIX, Mac, etc).
3. Es de dominio público (gratuito), aunque no todas sus versiones lo sean.
4. No ha sido desarrollado ni es controlado por ninguna organización gubernamental.
5. Esta basado en algoritmos extremadamente seguros:
   - Clave pública con clave variable: para cifrado de claves.
   - Algoritmo internacional de encriptamiento de datos: para cifrado del documento propiamente dicho.
6. Su manejo es sencillo e intuitivo.

7. Por sus prestaciones, las cuales son:

- Confidencialidad: permite a un usuario, mediante cifrado, garantizar que solamente el destinatario podrá leer el mensaje.
- Autentificación: permite a un usuario firmar un documento antes de enviarlo, lo cual permite: tener certeza de que el documento no ha sido modificado puesto que ha sido firmado, si se alterara el mensaje la firma no sería válida, verificar que el mensaje ha sido firmado por una determinada persona.
- Integridad: la firma antes mencionada tiene la particularidad de que depende no sólo de la identidad del remitente sino también del contenido del mensaje, por lo que si este es alterado, la firma ya no es válida.
- Otras: además de las posibilidades anteriormente citadas tiene otras de particular interés, como por ejemplo la posibilidad de encriptar ficheros o de asegurar un borrado permanente de estos.

CAPITULO V
SEGURIDAD CON AUTENTICACIÓN

La publicación de grandes volúmenes de información a través de Internet constituye un medio conveniente de tener acceso a esa información de una manera ágil y eficaz, contando además con disponibilidad global. Más aún, la posibilidad de crear un canal de comunicaciones bidireccional, gracias al cual los usuarios no sólo son capaces de recuperar información de un servidor web, sino también de transmitírsela, principalmente a través de formularios, representa una forma igualmente eficiente de suministrar datos personales e información privada desde cualquier lugar del mundo.

Sin embargo, nunca debería suministrarse información confidencial por Internet ni almacenarse en servidores web sin ningún tipo de protección, especialmente en lo que se refiere a datos financieros y comerciales sensibles. A medida que crece la cantidad de información públicamente disponible y transportada a través de Internet, también lo hace la necesidad de asegurarla en parte o en su totalidad, protegiéndola de escuchas pero no en la disminución de su facilidad de acceso.

La autenticación puede referirse a relaciones con usuarios de ordenadores (personas), máquinas (terminales), u objetos (programas). Con el método de autenticación a través de un análisis de riesgos, puede determinar que los riesgos asociados con el acceso no autorizado, descubrimiento, o modificación de datos no detectada justifican la implementación de medidas de seguridad que incluyen una combinación de métodos de protección de datos. Las redes conectadas a Internet deberían implementar funciones de autenticación que sean consistentes con el nivel de confidencialidad o sensibilidad de la información que contienen y procesan.

La autenticación es el procedimiento de verificar la elegibilidad de un usuario, máquina o componente de software para que acceda a categorías específicas de información.

La autenticación de usuarios verifica la identidad de cualquier persona que interactúa con un sistema informático. Esta verificación frecuentemente toma la forma de pedir a la persona que proporcione algo que se conoce como contraseña.

V.1 ALGUNOS PROTOCOLOS

Los protocolos emplean una serie de valores conocidos y permanentes, como los identificadores de las terminales de la red y otros que son números de un solo uso, generalmente aleatorios.

A continuación se exponen algunos ejemplos de protocolos, dando primeramente la lista de abreviaturas de los elementos que se van a utilizar en ellos:

A: identificador de Alicia, un usuario legítimo del sistema.
B: identificador de Benito, un usuario legítimo del sistema.
T: identificación de Teresa, una tercera parte confiable.
H: identificación de Hilario, un intruso de la red.
E: algoritmo de cifrado de clave simétrica.
K: clave secreta.
r_A, r_B: número pseudoaleatorio, generado por Alicia o Benito.
t_A, t_B: sello temporal, generado por Alicia o Benito.
n_A, n_B: número secuencial.

Protocolo de autenticación por desafío-respuesta.

A continuación se presenta uno de los protocolos más simples que se puede construir para que Alicia y Benito puedan demostrarse mutuamente su personalidad; este protocolo se muestra en la tabla V.1. Ambos comparten una clave secreta K y usan

un algoritmo de cifrado simétrico E. Se supone que la clave que comparten la han establecido mediante un procedimiento seguro. El protocolo consiste en intercambiar dos números aleatorios r_A y r_B para verificar mutuamente su identidad:

Etapa	Dato	OPERACIÓN	Flujo de información
1	r_A	A genera un número aleatorio r_A	A→B
2	$E_K(r_A, r_B)$	B genera r_B lo relaciona con r_A , cifra los números con el algoritmo E bajo la clave K, que envia a A	B→A
3	r_B	A recupera r_A y r_B, devuelve r_B a B	A→B

Tabla V.1 Protocolo desafío-respuesta

Primero, Alicia envía a Benito un número r_A Benito lo incluye en un mensaje relacionado junto con otro número r_B creado por él; a continuación cifra este mensaje con el algoritmo conocido por ambos, E, bajo la clave K y se lo envía a Alicia (respuesta). Alicia descifra el mensaje y recupera el número r_A de la respuesta de Benito, comprobando que habla con Benito. También recupera el número r_B, que envía a Benito. Éste recibe en la respuesta el número r_B descifrado; por tanto, sabe que habla con Alicia, pues sólo ella sería capaz de descifrar el mensaje.

Un protocolo tan sencillo podría ser atacado por Hilario, un intruso de la red, suplantando a Benito como se muestra a continuación en la tabla V.2:

Etapa	Dato	OPERACIÓN	Flujo
1	r_A	A inicia un protocolo con H creyendo que es B	A→H
2	r_A	H inicia un segundo protocolo con A fingiendo ser B	H→A
3	$E_K(r_A, r_A)$	A responde al segundo protocolo	A→H
4	$E_K(r_A, r_A)$	H responde al primer protocolo	H→A
5	r_A	A termina el segundo protocolo	A→H
6	r_A	H termina el segundo protocolo	H→A

Tabla V.2 Ataque de un intruso de la red al protocolo de desafío-respuesta

El resultado del ataque es que Hilario ha suplantado a Benito y ha iniciado dos sesiones de comunicación con Alicia.

Este ataque se pudo evitar si se hubiesen incluido ciertos parámetros de un solo uso, tales como números aleatorios, sellos temporales y números secuenciales.

Protocolo de autenticación con sello temporal

Una forma de impedir el ataque de Hilario seria hacer uso de un sello temporal. Seguidamente se presenta un esquema de protocolo de autenticación, que hace uso de un sello temporal tabla V.3.

Etapa	Dato	OPERACIÓN	Flujo de información
1	E_K (t_A, B)	A envía un sello temporal cifrado a B	A→B

Tabla V.3 Uso de un sello temporal

Benito comprueba, tras descifrar el mensaje, que el sello temporal es conveniente, que el identificador es el suyo y que Alicia conoce la clave; así Alicia queda autenticada frente a Benito. El sello temporal t_A evita un ataque por reenvío retardado contra Benito. El indicador de Benito, B, evita un ataque inmediato contra Alicia por reflexión. Este método es sumamente económico, ya que consigue la identificación segura con un solo mensaje.

Protocolo de autenticación de contraseña.

El protocolo de autenticación de contraseña utiliza contraseñas en texto simple (no cifradas) y es el protocolo de autenticación menos sofisticado. El protocolo de autentificación de contraseña se suele utilizar si la conexión y el servidor no pueden negociar una forma de validación más segura. Puede que se necesite utilizar este protocolo si se va a llamar a un servidor que ejecute un sistema operativo distinto de Windows.

Protocolo de autenticación por desafío mutuo.

El protocolo de autenticación por desafío mutuo intenta evitar las limitaciones del protocolo de autenticación de contraseña evitando mandar las contraseñas de forma que el intruso de la red no pueda tener acceso a ellas. El protocolo de autentificación

por desafío mutuo es un método el cual su principal función es la autentificar únicamente al usuario que se le van a enviar los datos, el protocolo de autenticación por desafío mutuo realiza los siguientes pasos:

1. El servidor manda al usuario una clave aleatoria, el usuario usa esta clave para encriptar la contraseña y devuelve la contraseña encriptada al servidor.
2. El servidor busca el nombre del usuario en la base de datos y toma la contraseña del servidor. El servidor entonces encripta la contraseña con la misma clave y compara el resultado con la respuesta del usuario.

Este protocolo es seguro contra intrusos de la red Internet. Cada vez que un usuario se conecta a la red, el sistema genera una clave aleatoria, por lo que la misma contraseña es encriptada de forma diferente cada vez. Mientras que el servidor no mande nunca al usuario la misma clave aleatoria, la contraseña encriptada que el intruso la pueda interceptar, nunca volverá a ser válida. El problema con el protocolo de autentificación por desafío mutuo es que la base de datos de las contraseñas en el servidor debe de estar en texto simple para permitir al servidor validar la respuesta del usuario replicando la encriptación que tiene lugar en la computadora del usuario.

Aunque el protocolo por desafío mutuo es un intento de ser más seguro que el protocolo de autenticación de contraseña, realmente lo único que hace es cambiar un tipo de seguridad por otro. Aunque la contraseña no se manda claramente, la base de datos del servidor es altamente vulnerable. Por lo tanto con el protocolo de autenticación de contraseña, el usuario consigue seguridad de la base de datos a cambio de seguridad de transmisión; y con el protocolo de autenticación por desafío mutuo, el usuario consigue seguridad de transmisión a cambio de seguridad de base de datos.

Protocolo punto a punto

El Protocolo Punto a Punto (PPP - Point to Point Protocol) fue diseñado para enviar datos a través de conexiones de punto a punto de marcación o a través de conexiones dedicadas. El protocolo punto apunto encapsula paquetes del protocolo de Internet, dentro de las tramas del protocolo punto a punto, y después los transmite a través de un enlace de punto a punto.

Hay cuatro fases de negociación en una sesión de marcación de protocolo punto a punto, cada una de estas debe completarse satisfactoriamente antes de que la conexión de punto a punto esté lista para transferir los datos del usuario. Estas fases son las siguientes:

1. Establecimiento del enlace de punto a punto: el protocolo de punto a punto utiliza un protocolo de control de enlace para establecer, mantener y terminar la conexión física. Tomando en cuenta que durante esta fase de establecimiento del enlace, se seleccionan los protocolos de autenticación, pero no se implementan realmente hasta la fase de autenticación de usuarios, la fase 2.
2. Autentificación de usuarios: en esta fase, la computadora que hace de cliente presenta la identificación del usuario al servidor de acceso remoto. Esta fase de autentificación proporciona protección contra los ataques de contestación e imitación de clientes remotos.
3. Control de retorno de llamada de punto a punto: la implementación del protocolo de punto a punto incluye una fase opcional de control de retorno de llamada. Esta fase utiliza el protocolo de control de retorno de llamada inmediatamente después de la fase de autenticación. Si la configuración es para retorno de llamada, después de la autenticación el cliente remoto se desconecta.
4. Petición de protocolos de nivel de red: en esta fase, el protocolo punto a punto utiliza los protocolos de control de red que fueron seleccionados durante la fase de establecimiento del enlace para configurar los protocolos utilizados por el cliente remoto.

Protocolo de autenticación extensible.

El protocolo de autenticación extensible (EAP - Extensible Authentication Protocol) es una extensión del protocolo punto a punto (PPP - Point to Point Protocol). El protocolo de autenticación extensible se desarrolló como respuesta al aumento de la demanda de autenticación de usuarios de acceso remoto que utilice otros dispositivos de seguridad. Este protocolo proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con el protocolo punto a punto. Al utilizar el protocolo de autenticación extensible, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes y certificados. El protocolo de autentificación extensible, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN - Virtual Private Network), puesto que ofrece mayor seguridad frente a ataques físicos y de investigación de contraseñas que otros métodos de autenticación, como el protocolo de autenticación por desafío mutuo.

V.2 SERVICIOS DE MARCACIÓN PARA USUARIOS REMOTOS

Los empleados de las empresas desean cada vez más poder trabajar lejos de sus oficinas, ya sea en sus casas u otros lugares. El personal de ventas desea cada vez más poder accesar bases de datos y los administradores desempeñar sus funciones desde ubicaciones remotas.

De acuerdo a la importancia que han recobrado las redes, la capacidad de las personas para marcar y tener acceso a redes cada vez es más importante. Con el servicio de marcación para usuarios remotos, las empresas pueden expandir sus redes a líneas telefónicas.

El servicio de marcación para usuarios remotos es un método basado en el protocolo de datagrama de usuario para administrar la autenticación y autorización de usuarios remotos. Los servidores este servicio pueden localizarse en Internet y proporcionan autenticación incluyendo protocolo punto a punto, protocolo de autenticación de contraseña, protocolo de autenticación por desafío mutuo, y el protocolo de autenticación extensible.

El servicio de marcación para usuarios remotos, (RADIUS - Remote Authentication Dial-In User Service) es un protocolo estándar del sector RFC 2138 y 2139, para suministrar servicios de autenticación, autorización y cuentas al acceso telefónico a redes distribuidas. Un cliente que cuenta con este servicio, normalmente un servidor de acceso telefónico utilizado por un proveedor de servicios Internet (ISP - Internet Service Proveer), envía información de conexión y de usuario a un servidor. El servidor autentifica y autoriza la solicitud del cliente. Este protocolo estándar fue descubierto por compañía Livingston Enterprises como un servicio de autenticación de acceso que puede ser usado por varios proveedores de servicios de Internet para autentificar a sus usuarios.

En el caso de un servidor de acceso remoto con plataforma Windows 2000 incluye un cliente con este protocolo de manera que el proveedor de servicios Internet o los usuarios corporativos de acceso remoto, que utilizan este protocolo como esquema de cuentas o autenticación, puedan utilizar el servidor de acceso remoto.

Este protocolo puede configurar los proveedores de cuentas y autenticación del servidor de acceso remoto de Windows 2000 de manera independiente. Por lo tanto, un servidor de acceso remoto puede utilizar Windows 2000 como proveedor de autenticación y como proveedor de cuentas.

A continuación se muestra en la figura V.1 como se utiliza el servicio de marcación para usuarios remotos en ambiente Windows 2000.

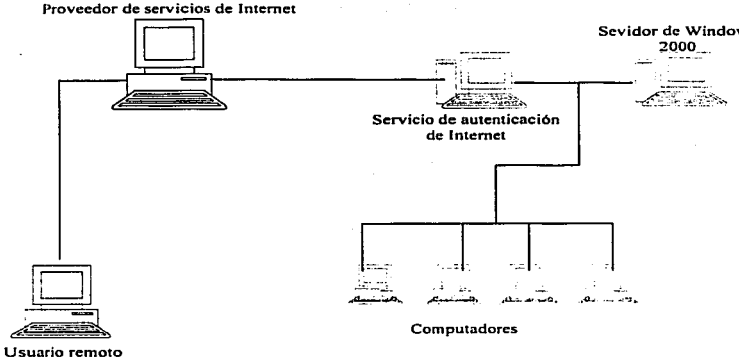


Fig. V.1 Protocolo de servicio de marcación en ambiente Windows 2000

Primero el usuario remoto marca dentro del sistema de su proveedor de servicios de Internet. Pero el proveedor de servicios de Internet no puede hacer una determinación de autenticación de usuario, por eso hace una petición al servicio de autenticación de Internet que es el que determina que tipo de servicio requiere el usuario remoto. El servicio de autenticación de usuario provee la autenticación al usuario remoto y así este puede activar una sesión con la red.

Los sistemas de marcación para usuarios remotos de la compañía de sistemas Cisco cuentan con las siguientes características:

- Este servicio utiliza el protocolo de datagrama de usuario.
- Para autenticación, este servicio encripta solo la contraseña entre el cliente y el servicio de marcación.
- Este servicio no soporta múltiples protocolos y trabaja solo en redes de protocolo de Internet.
- Este servicio no tiene la habilidad para controlar los comandos que son ejecutados en un ruteador.

V.3 SISTEMAS DE CONTROL DE ACCESO PARA TERMINALES

El termino de control de acceso denota típicamente el tipo de acceso permitido. Tipo de acceso se refiere en este caso a leer, escribir, ejecutar, borrar, controlar, actualizar, o todos. Los recursos pueden incluir ficheros, objetos de red, sistemas informáticos, etcétera. Control de acceso también se refiere a las tareas de seguridad desarrolladas por hardware, software y controles administrativos para monitorear una operación de sistema, asegurar la integridad de los datos, realizar la identificación de usuarios, registrar accesos y cambios del sistema, y conceder acceso a los usuarios.

Los sistemas de control de acceso son un protocolo de autenticación propiedad de la compañía de sistemas Cisco, desarrollado para suministrar autenticación de acceso remoto, como por ejemplo, el registro de eventos. Las contraseñas de usuario se administran en una base de datos central en lugar de administrarse en ruteadores individuales, suministrando una solución de seguridad de red. Estos sistemas permiten el servicio de acceso remoto para comunicarse con un servicio de autenticación para saber si el usuario tiene acceso a la red.

Los sistemas de control de acceso fueron desarrollados en 1989 y a medida que paso el tiempo estos sistemas de control de acceso fue evolucionando hasta tener otra versión llamada sistema de control de acceso mejorada. Esta versión tiene las siguientes características:

- Los sistemas de control de acceso mejorado a diferencia de los sistemas anteriores no utiliza protocolo de datagrama de usuario, este utiliza protocolo de control de transmisión.
- Estos sistemas mejorados pueden encriptar el paquete entero, protegiendo también la contraseña, el nombre de usuario y otra información entre el cliente de Cisco y el servidor. La comunicación de la estación de trabajo al cliente Cisco que provee servicios de acceso no esta encriptada.
- Los sistemas de control de acceso soportan múltiples protocolos uno de ellos es el protocolo de Internet.

Los sistemas de control de acceso se pueden encontrar en tres versiones distintas, las cuales son: sistemas de control de acceso para terminales (TACACS – Terminal Access Controler Access Control System), los sistemas de control de acceso para terminales extendidos (XTACACS – Extended Terminal Access Controler Access Control System), y los sistemas de control de acceso para terminales mejorados (TACACS+ - Terminal Access Controler Access Control System Plus), a continuación se mencionan algunas de las diferencias entre cada una de estas versiones.

- Los sistemas de control de acceso para terminales son sistemas habilitados para peticiones de autenticación únicamente.
- Los sistemas de control de acceso para terminales extendidos tienen la habilidad de realizar elementos de autenticación, autorización e identificación.
- Los sistemas de control de acceso para terminales mejorados realiza todo lo anterior pero utiliza el protocolo de control de transmisión.

V. 4 SISTEMAS DE DISTRIBUCIÓN DE CLAVES

El sistema de distribución de claves, fue desarrollado en el Instituto de Tecnología de Massachussets para proteger los servicios de red que surgieron con el proyecto Athena. El objetivo del sistema de distribución de claves fue extender la noción de autenticación, autorización e identificación del entorno de computación y de red del Instituto de Tecnología de Massachussets. De acuerdo al plan técnico de Athena, este entorno estaba formado básicamente por:

- Estaciones de trabajo públicas y privadas.
- Las estaciones públicas se localizan en áreas sin seguridad o con solo seguridad mínima.
- Las estaciones privadas están bajo control físico y administrativo de individuos generalmente sin responsabilidad de administradores centrales de red.
- Una red de área limitada, formada por redes de área local (LAN- Local Área Network) de distintas topologías conectadas a una red troncal. Las redes de área local están dispuestas en lugares dispersos, y son vulnerables a diversos ataques.
- Servidores operados centralmente. La mayor parte están situados en habitaciones cerradas, y funcionan por tanto en condiciones de seguridad física moderada, con software que no contiene código malicioso.

Este entorno no es apropiado para almacenar, procesar o transmitir datos confidenciales, como registros financieros o datos clasificados, ni para realizar operaciones de alto riesgo, como el control de un experimento peligroso. Los riesgos existentes son principalmente debidos al uso incontrolado de recursos por parte de entidades no autorizadas, violaciones de la integridad de los recursos del sistema y violaciones masivas de la privacidad, como por ejemplo, la visualización de archivos.

En este entorno, las amenazas principales a la seguridad surgen de la posibilidad de que el usuario de una estación de trabajo falsifique la identidad de otro usuario para obtener acceso no autorizado a los recursos del sistema.

Las primeras tres versiones del sistema de distribución de claves se utilizaron solo en el Instituto de Tecnología de Massachussets. La primera versión disponible para uso público fue la versión 4 (V4).

En 1989 se comenzó a trabajar en la versión 5 del sistema de distribución de claves. El trabajo se llevo a cabo debido al resultado de las discusiones entre usuarios y administradores de la versión 4. En Septiembre de 1993, la versión 5 del sistema de distribución de claves se especifico como un protocolo de seguimiento de estándares en Internet, en el documento RFC 1510.

En terminología del sistema de distribución de claves, los dominios de administración se denominan reinos. Se supone que toda compañía u organización que desee utilizar este sistema establecerá un reino particularmente determinado por un nombre de reino. En teoría, cada reino del sistema de distribución de claves puede admitir hasta 100 000 usuarios.

El sistema se basa en el modelo cliente / servidor. Los usuarios, los clientes y los servicios de red ejecutándose en sistemas concretos se consideran generalmente principales. Cada principal se identifica mediante un único identificador principal.

El objetivo del sistema de distribución de claves es permitir que un cliente ejecutándose en nombre de un usuario particular pruebe su identidad a un servicio o al correspondiente servidor de aplicaciones sin necesidad de enviar datos por la red que podrían facilitar el que un intruso suplantase posteriormente al usuario. Para conseguir

este objetivo, el modelo de distribución de claves requiere la existencia de una entidad de confianza que actué como centro de distribución de claves (KDC- Key Distribution Center). El centro de distribución de claves consta de dos componentes:

1. Un servidor de autenticación (AS - Authentication Server).
2. Un conjunto de servidores de emisión de etiquetas (TGS- Ticket Granting Servers).

Un servidor de autenticación y los servidores de emisión de etiquetas son solo componentes separados lógicamente, y pueden ser, por ejemplo, procesos ejecutándose en los mismos sistemas. Debe también advertirse que los sistemas que proporcionan estos servicios deben estar cuidadosamente protegidos y ser físicamente seguros.

El sistema de distribución de claves proporciona varias herramientas para la gestión de la base de datos del centro de distribución de claves. Las funciones de gestión se realizan de forma remota por la red, y el propio sistema de distribución de claves autentifica las conexiones a la base de datos del centro de distribución de claves. Las actualizaciones se realizan mediante un protocolo que se ejecuta entre un cliente autentificado en una estación de trabajo y la base de datos del centro de distribución de claves. Existen rutinas de actualización para añadir y desactivar entradas principales y para dar soporte a los cambios de contraseñas iniciados por el administrador o por el usuario. La figura V.2 muestra el modelo básico del sistema de distribución de claves.

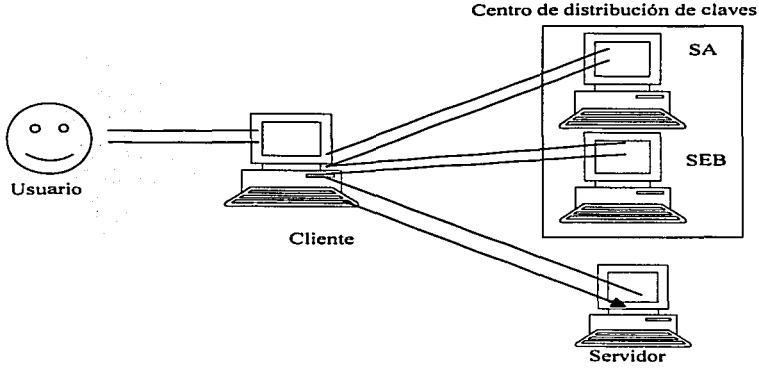


Fig. V.2 Modelo básico del sistema de distribución de claves.

En el centro de la figura, un cliente se está ejecutando en el nombre del usuario. Para poder utilizar los servicios del servidor que se muestra en la parte inferior derecha de la figura, el cliente se debe de autentificar ante dicho servidor.

En esta situación el centro de distribución de claves de nuestro sistema debe proporcionar al cliente las claves que debe de utilizar en el intercambio de autentificaciones. Es importante darse cuenta de que ni el cliente ni el servidor comparten inicialmente una clave de sesión. Siempre que un cliente se va a autentificar ante a un servidor, el centro de distribución del sistema debe generar una clave de sesión y transmitírsela de forma segura a las entidades involucradas.

V. 5 CERTIFICADOS

Los certificados son un conjunto de datos utilizado para la autenticación y el intercambio seguro de información en redes no seguras, como Internet. Los certificados de clave pública o identificadores digitales, son mecanismos digitales similares a las tarjetas de identidad o a los pases de seguridad de los empleados que pueden utilizarse para verificar la identidad de alguien en Internet. Los certificados son un método más seguro que el nombre de usuario y su contraseña, y son apropiados cuando se ejecutan aplicaciones de Internet como el correo electrónico encriptado y acceso de un solo usuario a múltiples servidores del Internet.

Un certificado enlaza de forma segura una clave de cifrado pública con la entidad que guarda la clave de cifrado privada correspondiente. La entidad emisora de certificados firma digitalmente los certificados, que pueden ser administrados por un usuario, un equipo o un servicio. El formato aceptado de forma más generalizada para los certificados está definido por la norma X.509. Los certificados X.509 son archivos que contienen distintos campos donde se almacena la clave pública de un usuario, la firma de esa clave pública, información sobre los algoritmos criptograficos utilizados, datos identificativos del usuario y datos de la autoridad certificadora que ha firmado la clave para permitir comprobar su autenticidad. El esquema general se muestra en la figura V.3.

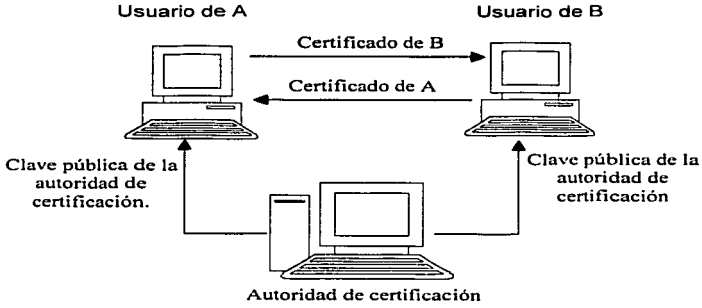


Figura V.3 Esquema general de autenticación mediante certificados de clave pública

V. 6 TARJETAS INTELIGENTES

Las tarjetas inteligentes se desarrollarón en el año 1983. Su función es muy sencilla, se trata de almacenar información con una cierta autonomía. Aunque la cantidad de información que pueden almacenar es relativamente pequeña, su autonomía es lo suficientemente importante como para haber producido la expansión de este tipo de tarjetas en el mercado. Las tarjetas inteligentes se han convertido en elementos importantes en campos tales como el dinero electrónico, el control de acceso e identificación. Algunas de los servicios que ofrecen estas tarjetas son:

- Autenticación a nivel de cliente.
- Protección de datos.
- Administración de sistemas.

La tarjeta inteligente es básicamente un chip, colocado en un rectángulo de un material plástico de aproximadamente 85 x 54 mm. Las tarjetas se suministran habitualmente en color blanco, pero pueden ser impresas utilizando diferentes sistemas. El chip que contiene dispone de unos contactos exteriores que son los que le permiten mantener una comunicación con sus circuitos, y de esta forma tener acceso a la información que contiene o grabar nueva información. Estos contactos están bañados en oro para que la tarjeta sea resistente a un uso habitual en cualquier tipo de entorno como lo puede ser la alta humedad (incluso con condensación). Su pequeño formato hace que sea ideal como sistema de identificación personal. Además, su medida no está limitada por razones técnicas, sino por razones de estandarización, es decir, técnicamente se podrían utilizar tarjetas que fuesen la cuarta parte del tamaño de las actuales.

Las tarjetas inteligentes han sido desarrolladas como sistema de almacenamiento de información inteligente e interactivos. Por lo tanto, su uso abarca desde sistemas de moneda electrónica, hasta sistemas de identificación asociados al almacenamiento de información de los elementos a identificar. Debido a su capacidad de modificar el contenido sin el requerimiento de un grabador excesivamente costoso y la capacidad de realizar múltiples grabaciones sin riesgo de perdida de la información, están desechando a las tradicionales tarjetas de banda magnética. Además, las tarjetas inteligentes microprocesadas permiten tener un control mucho más seguro sobre la identificación, de forma que tras acuerdos internacionales entre fabricantes, existen identificadores diferentes para todas las tarjetas que circulan por el mundo.

Existen básicamente dos grandes grupos de tarjetas inteligentes, las cuales son:

1. Tarjetas microprocesadas: Tienen como principal utilidad el uso de sistemas de tarjetas monedero, tarjetas de telefonía, etc;. y de identificación de alta seguridad. Su gran uso en la banca ha permitido una rebaja constante en su precio. Normalmente no

permiten almacenar mucha información, ya que su uso requiere generalmente poca cantidad de datos. Éstas disponen de una zona de memoria protegida, solo accesible por el fabricante, que garantiza una identificación única a nivel universal.

2. Tarjetas de memoria: Sustituyen la complejidad del sistema de seguridad por una mayor capacidad de almacenar datos. Estas tarjetas permiten la lectura y grabación de datos con las funcionalidades que esto implica. Actualmente se están fabricando tarjetas de hasta 32 Kb. de memoria. Evidentemente, la capacidad de almacenamiento está directamente relacionada con su costo.

Al ser gravables en su totalidad, estas tarjetas no garantizan la autenticación con absoluta seguridad, por lo que se ha de recurrir a sistemas de encriptación propios de la aplicación con la que la tarjeta ha de operar.

Una de las características más importantes de las tarjetas inteligentes es que estas permiten el traslado seguro de información privada entre varios sistemas.

La industria de las tarjetas inteligentes está plagada de incompatibilidades entres sus diferentes aplicaciones. La ausencia de un modelo estándar que regule la comunicación entre las terminales de lectores y ordenadores, que definiera las interfaces independientes de la terminal del lector para el desarrollo de aplicaciones, ha limitado el uso de soluciones basadas en tarjetas.

Las tarjetas inteligentes presentan bastantes ventajas en comparación con las tarjetas de banda magnética, las cuales son:

- Son capaces de almacenar mayor cantidad de información.
- Pueden proteger la información que almacenan en sus memorias de posibles accesos no autorizados.
- Poseen una mayor resistencia al deterioro de la información almacenada.

Dado que el acceso a la información realizada a través de un puerto serie y supervisado por el propio sistema operativo de la tarjeta, es posible escribir datos confidenciales que no puedan ser leídos por personas no autorizadas. En principio, las funciones de escritura, lectura y borrado de la memoria pueden ser controladas tanto por hardware como por software, o por ambos a la vez.

Como ya se ha mencionado las tarjetas inteligentes poseen un chip, este a su vez contiene un pequeño microprocesador que además cuenta con algunos elementos adicionales como lo son:

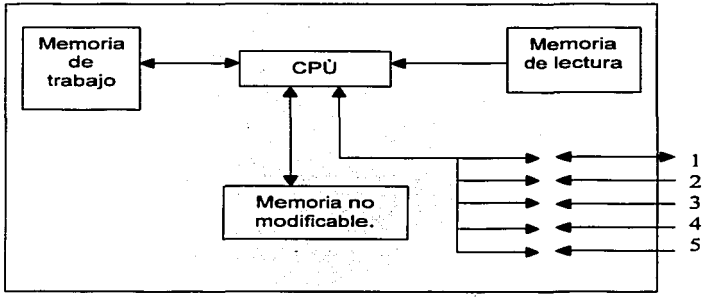
- La memoria de lectura, tiene el sistema operativo de la tarjeta y se graba durante el proceso de fabricación

- La memoria que no se puede modificar del microprocesador, en ella se encuentran datos del usuario o de la aplicación, así como el código de las instrucciones que están bajo el control del sistema operativo. También pueden contar con la información tal como el nombre del usuario y el número de identificación personal.

- La memoria de trabajo del microprocesador. Al ser modificable, toda la información se pierde al desconectar la alimentación.

Las tarjetas con microprocesador son bastante flexibles puesto que pueden realizar bastantes funciones. En el caso más simple, solo contiene datos referentes a una aplicación especifica, esto hace que dicha tarjeta sólo se pueda emplear para esa aplicación, sin embargo, los sistemas operativos de las tarjetas más modernas hacen posible que se pueda integrar programas para distintas aplicaciones en una sola tarjeta. En este caso, la memoria de lectura contiene solo el sistema operativo con las instrucciones básicas, mientras que el programa específico de cada aplicación se graba en la memoria no modificable después de la fabricación de la tarjeta y la tarjeta de memoria de trabajo se encuentra en uso mientras la tarjeta se encuentra conectada a la

fuente de alimentación. En la figura V.4 se presenta la arquitectura típica de una tarjeta inteligente.



1 Entrada/salida
2 Reloj
3 Reinicio
4 Alimentación
5 Tierra (GND)

Fig. V.4 Arquitectura típica de una tarjeta inteligente con microprocesador

CONCLUSIONES

- Se ha mencionado algunos de los métodos más comunes para proteger los datos a través de la red Internet, algunos problemas cruciales de la seguridad y algunas de las amenazas y ataques a la red más comunes.

- Es importante establecer las necesidades de seguridad en el envío de datos de cualquier usuario, o empresa, para poder determinar las posibles soluciones o los posibles métodos que se pueden emplear.

- No existe un método que garantice al 100% la seguridad en el envío de datos a través de la red Internet debido a las diferentes formas con que se puede romper la seguridad de un sistema de computo.

- Se puede llevar a cabo una buena planeación de los métodos que se deseen utilizar para obtener una mayor seguridad en el envío de datos, lo cual puede tener como consecuencia desde la salvación de una empresa hasta la obtención de ganancias económicas, o la confiabilidad y la seguridad en red de una empresa.

- Uno de los objetivos principales que se planteo al inicio de este proyecto de tesis y que se cumplió, es el de reducir al mínimo, con los métodos planteados, los riegos de que un intruso de la red Internet obtenga información que no le corresponde, implementando adecuadamente los diferentes métodos de seguridad mencionados en el envío de datos a través de la red Internet.

- Es importante conocer las posibles amenazas y ataques a la red Internet para poder tener una percepción más clara en las posibles consecuencias que se pueden llegar a tener, como lo son las grandes pérdidas económicas en una empresa o la intercepción o alteración de datos sumamente importantes por correo electrónico; e implementar el método de seguridad en el envío de datos que mejor le parezca al

usuario o a la empresa para estar seguros de que los datos enviados o recibidos estén intactos.

- Se debe usar un método de seguridad y de detección de intrusos basado en un computador en el servidor de Internet para proteger información como los nombres de clientes, las direcciones, el registro de compras, la información de las tarjetas de crédito, información secreta, etcétera.

- Hay que establecer métodos de autenticación para las conexiones por la red Internet, con base en el valor de la información que está disponible a través de la conexión.

- La mayoría de los métodos mencionados se basan principalmente en el uso de claves públicas, o claves privadas, o la combinación de los dos tipos de claves, con el propósito de tener una mayor seguridad al enviar o recibir datos.

- Existen diferentes tipos de amenazas que pueden comprometer la seguridad en el envío de datos a través de la red Internet, para evitar estas amenazas se han desarrollado métodos, protocolos y aplicaciones que utilizan técnicas criptográficas, de cifrado, y de autentificación, las cuales se han mencionado en este proyecto de tesis.

- En este proyecto de tesis se hace mención de los métodos de seguridad en el envío de datos a través de la red Internet, desde los primeros en utilizarse en la red Internet que son a diferencia de otros fáciles de implementar, nos referimos al cifrado con sus distintas formas de implementarse, desde el convencional pasando por clave pública y privada hasta el cifrado con clave variable. Pasando por los métodos más utilizados en la actualidad como lo es la seguridad con el protocolo de Internet y con encriptamiento, hasta el método más actual que es la autenticación con tarjetas inteligentes.

GLOSARIO

Algoritmo

Método y notación de las distintas formas del cálculo aritmético y algebraico. Un algoritmo criptográfico es una función matemática que combina texto simple u otra información inteligible con una cadena de dígitos, llamada clave, para producir texto codificado ininteligible.

ARPA

Advance Research Projects Agency, Agencia de Proyectos Avanzados de Investigación.

Arquitectura de comunicaciones

Son las estructuras de hardware y software que implementan las funciones de comunicación.

ASCII

American Standard Code for Information Interchange, Código Normalizado Americano para el Intercambio de Información. Se trata de un código que se asigna a cada letra, número o signo empleado por los computadores, una combinación de ceros y unos. Es el código más utilizado por todos los computadores a nivel internacional. El código ASCII le asigna 8 bits a cada carácter.

Autenticación o Autentificación

Es la verificación de la identidad del emisor, quien genera el mensaje, y la integridad de los datos.

Bits

Es la unidad más pequeña de información. Un bit puede tomar el valor 0 o el valor 1. Los computadores internamente solo pueden manejar este tipo de información.

Cabecera

Información del control de un sistema definido que procede a los datos del usuario.

Cajas-S

Cadena de bits que pueden representarse por los valores en hexadecimal.

Cifrado

Convertir textos puros o datos en una forma ininteligible mediante el uso de un código de forma que posteriormente se pueda hacer la reconversión a la forma original.

Cifrado Asimétrico

Un método de cifrado en el que el cifrado y descifrado se realizan usando dos claves diferentes, una de ellas llamada clave pública y la otra clave privada. También se conoce como cifrado de clave pública.

Cifrado Simétrico

Un tipo de sistema criptográfico en el que el cifrado y descifrado se realizan usando la misma clave. También se conoce como cifrado convencional.

Clave

Explicación de los signos para escribir en cifra.

Clave Privada

Una de las dos claves usadas en un cifrado asimétrico. Para una comunicación segura, el creador de la clave privada debe ser el único que la conozca.

Clave Pública

Una de las dos claves usadas en un sistema de cifrado asimétrico. La clave pública se hace pública, para ser usada junto con su correspondiente clave privada.

Confidencialidad

Es la protección de los datos enviados para no ser revelados a aquellos usuarios que no deben recibir la información.

Conmutación de paquetes

La conmutación de paquetes es un sistema de comunicación de datos mediante el cual toda la información que sale de un terminal para ser transmitida por la red de conmutación de paquetes es dividida en bloques de una determinada longitud. A cada paquete se le añade la información necesaria al comienzo del mismo paquete, de manera que cada paquete se pueda mover por la red de forma independiente. Si en un momento dado una ruta o un nodo de comunicaciones queda fuera de servicio, los paquetes que en un principio utilizaban estos medios son enviados de forma automática por otras rutas, sin que quede interrumpida la comunicación.

Computador

Es un dispositivo que se utiliza para enviar o recibir datos dentro de una red.

Correo Electrónico

Es una aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. En Internet, el correo electrónico o e- mail permite que todos los usuarios conectados a ella puedan intercambiar mensajes.

Criptografía

Es la ciencia o el arte de escribir con clave secreta o de un modo enigmático.

DARPA

Defense Advanced Research Projects Agency, Agencia de Proyectos Avanzados de Investigación para la Defensa, se trata de una agencia de investigación del departamento de defensa de los Estados Unidos.

Datagrama

Es un paquete individual de datos que se envía al computador receptor sin ninguna información que lo relacione con ningún otro posible paquete enviado. El procedimiento de datagramas se suele usar cuando los datos a transmitir son pocos.

Datos

Representación de la información o mensajes mediante bits, ceros y unos.

DEA

Data Encryption Algorithm, Algoritmo de Cifrado de Datos.

Descifrado

La traducción de un texto o datos cifrados (o texto encriptado) al texto o datos originales (o texto puro). También se llama desencriptado.

Driver

Es un programa que hace de comunicación entre el software de la red y el hardware de la tarjeta de red instalada.

Emisor

Persona o usuario que manda datos a otra persona llamada receptor.

Encriptamiento

Es el proceso para codificar o proteger datos que no se quiere que sean leídos o interceptados por otras personas ajenas.

Enmascarar

Ocultar una determinada información de carácter confidencial.

Estándar

Definen las evoluciones de la tecnología que se utilizan para las comunicaciones.

Extranet

Es una red de control de acceso a los recursos del Internet que está disponible sólo a usuarios específicos.

Firma Digital

Mecanismo de autentificación que habilita al creador de un mensaje adjuntar un código que actúa como firma. La firma garantiza la fuente y la integridad del mensaje.

FTP

File Transfer Protocol, Protocolo de Transferencia de Archivos, es una aplicación de Internet que permite transferir archivos de un computador a otro. Las siglas FTP también pueden hacer referencia al propio protocolo.

Gateway

También llamado pasarela, es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí.

Hardware

Dispositivos físicos que comprende un sistema de computación.

Host

Es un computador que se utiliza para enviar o recibir datos dentro de una red.

ICMP

Internet Control Message Protocol, Protocolo de Control para Mensajes de Internet.

IETF

Internet Engineering Task Force, Grupo de Ingeniería en Internet, es una organización del consejo de la arquitectura Internet, cuya finalidad es discutir y dar solución a los posibles problemas técnicos que pueda tener Internet.

IKE

Internet Key Exchange, Intercambio de Claves de Internet.

IKMP

Internet Key Management Protocol, Protocolo de Gestión de Claves para Internet.

Integridad

Seguridad o afirmación de que los datos que tiene el receptor son los mismos que envió el emisor.

Internet

Es un conjunto de redes de ámbito mundial conectadas entre sí mediante el protocolo IP. A través de Internet se puede acceder a servicios como transferencia de archivos, acceso remoto, correo electrónico y noticias, entre otros.

Intranet

Es una red dentro de una organización o empresa que utiliza tecnologías de Internet que permite a sus empleados de la empresa buscar y compartir documentos, a una Intranet no puede tener acceso el público en general.

IP

Internet Protocol, Protocolo Internet, es el protocolo de nivel de red usado en Internet. Mediante el protocolo IP, cualquier paquete puede viajar a través de las distintas redes de Internet hasta llegar a su destino final. Registra las direcciones de nodos, encamina los mensajes que se envían y reconoce los mensajes recibidos.

IPsec

Internet Protocol Security, Seguridad con el Protocolo de Internet, es un conjunto de recomendaciones y protocolos para proteger intercambio de datos sobre IP, permitiendo una seguridad de extremo a extremo.

ISO

International Standard Organization, Organización Internacional para la Normalización, esta organización ha definido los protocolos de comunicaciones conocidos como ISO/OSI, utilizados para las redes públicas de conmutación de paquetes.

Kbps

Unidad de medida de la velocidad de transmisión de datos por un medio, indica el número de bits que se transmiten en un segundo (bps .- bits por segundo) por ese medio, como puede ser por línea telefónica, fibra óptica, etc,. La letra K es para expresar que es la unidad de mil (Kilos)10^3, tambien puede ser M (Megas)10^6, G (Gigas) 10^9, etc,.

Matriz

Se le llama matriz a todas las redes de computadores que intercambian correo electrónico. Una de las redes que forman la matriz es la red Internet, pero existen otras, como Compuserver, Bitnet, etc.

MIME

Multipurpose Internet Mail Extensions, se trata de un nuevo estándar de correo electrónico desarrollado para permitir enviar no sólo archivos de texto, sino también gráficos y sonidos por el correo electrónico. Otra característica de MIME es que permite darle distintos formatos a las letras.

Módem

Es un equipo que se conecta al computador para poder transmitir datos por una linea de transmisión. El módem suele ser utilizado en las comunicaciones de datos por línea telefónica, con una velocidad de transmisión entre 1200 y 19200 bits por segundo (bps).

Nodo

Se llama nodo al punto en común que tienen los computadores para conectarse directamente a una red.

Norma

Conjunto de reglas que deben seguir ciertos enlaces para llevar a cabo la comunicación.

OSI

Open Systems Interconnect, Interconeción de Sistemas Abiertos, se trata de una serie de protocolos normalizados por la Organización Internacional para la Normalización (ISO).

Paquetes

En una red, los datos transmitidos por un computador son divididos en conjuntos de caracteres independientes que reciben el nombre de paquetes. Cada paquete viaja por la red independientemente de los demás hasta llegar al destino. El tamaño de los paquetes puede variar entre 40 y 32 000 bits, aunque normalmente no tienen tamaños superiores a 1 500 bits.

Pasarela

Es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí.

Plataformas o Sistemas Operativos

Un sistema operativo es un programa traductor, el cual prepara y activa a un computadora para la ejecución de todas las aplicaciones y programas de software. Algunos ejemplos de sitemas operativos son: Windows 95/98/NT/2000/XP, Solaris, Mac, MacOS, Linux, UNIX.

Programas de correo electrónico

Los programas son instrucciones estructuradas y ordenadas de manera que al ser ejecutadas, hagan que la computadora realice una función particular, algunos programas de correo electrónico son: Eeudora, Eudora-Pro, Qualcomm, OnNet, Outlook, Messanger, McAfee.

Protocolo

Es un conjunto de normas que indican cómo deben actuar los computadores para comunicarse unos con otros.

Receptor

Persona o usuario quien recibe los datos enviados por el emisor.

Red

Una red es una configuración de computadores conectados entre sí utilizada para ligar un amplio rango de sistemas.

Red LAN

Local Area Network, Red de Área Local, es una red localizada que tiene un computador central, llamado servidor, que proporciona interconexión entre varios dispositivos de comunicación de datos en un área pequeña y servicios a múltiples nodos asociados, llamados clientes.

Red WAN

Wide Area Network, Red de Área Extensa, es una red formada por nodos conectados en un área geográfica extensa.

RFC

Request For Comments, Petición de Comentario, al principio, las reglas de comunicaciones de Internet no estaban muy especificadas, por lo que eran los propios usuarios los que hacían sugerencias de modificación o de nuevos protocolos. A estas

sugerencias se les llamo RFC. Hoy en día las RFC definen las normas de comunicación de Internet. Estas normas están numeradas a partir del número 1000.

Ruteadorr

También llamado router, es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o una combinación de ambos.

Seguridad

Es la calidad o el estado de estar libre de cualquier daño, también son las medidas de protección tonadas contra el espionaje, el sabotaje, el crimen, el ataque o la fuga.

Servidor

Se trata de un software instalado en un computador, llamado remoto, que le permite ofrecer un servicio a otro computador, llamado local.

Sistema

Designación colectiva que denota todo el hardware interconectado de computación, incluyendo procesadores, dispositivos de almacenamiento, dispositivos de entrada y salida, y el equipo de comunicaciones.

Software

Programas utilizados para dirigir las funciones de un sistema de computación.

SSL

Secure Sockets Layer, Capa de Socket Segura, es un protocolo de seguridad que proporciona la encriptación de datos, servicios de autenticación e integridad de mensajes.

TCP

Transmisión Control Protocol, Protocolo de Control de Transmisión, es un conjunto de protocolos de los niveles de red y transporte del modelo OSI que permite el intercambio de datos de computadores conectados a Internet.

Topología

Es la forma física o los patrones de conexión entre los dispositivos que integran la red, dicha conexión puede ser en estrella, anillo, bus, árbol, malla.

UDP

User Datagram Protocol, es un protocolo sobre el que funcionan ciertos servicios de Internet, se utiliza cuando se necesita transmitir voz o video donde es más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

Unix

Es un sistema operativo multitarea y multiusuario. Este sistema operativo aunque fue muy importante en el desarrollo de Internet, no es necesario saber utilizarlo para usar Internet.

Virus

Es una pieza de código de programación que se une a un programa y puede provocar una acción no deseada por los usuarios cuando éstos acceden a dicho programa. Algunos virus pueden actuar de forma inofensiva, pero otros pueden causar daños, como borrar o modificar archivos.

VPN

Virtual Private Network, Red Privada Virtual, es un tipo de red que ofrece un servicio de conexión segura y fiable sobre una red pública, un medio compartido.

World Wide Web

También conocido como www, es un sistema utilizado para localizar y acceder a las fuentes de información de Internet. Es un protocolo que permite a los usuarios hacer que su información sea fácilmente accesible para los otros usuarios. El www es un sistema cliente/servidor que soporta referencias de hipertextos.

X.25

Es un protocolo de transmisión de red de paquetes ISO utilizado en muchas redes de área extensa. Forma parte del modelo OSI.

X.400

Es un protocolo estándar ISO para enviar mensajes de una red a otra. Forma parte del modelo OSI.

BIBLIOGRAFÍA

- Cisco Network Security.
  Russell Lusignan, Oliver Steudler, Jacques Allison.
  Edit. Syngres

- Computer Networks and Open Systems.
  Lillian N. Cassel, Richard H. Austing.
  Edit. Jones and Bartlett Publishers

- Comunicaciones y Redes de Computadoras.
  William Stallings.
  Edit. Prentice Hall

- Secure Computers and Networks. Analysis, design, and Implementation.
  Eric A. Fisch, Gregory B. White.
  Edit. Prentice Hall

- Técnicas Criptográficas de Protección de Datos.
  Amparo Fuster S., Dolores de la Guía Martínez, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muños Masque.
  Edit. Alfa Omega Ra - ma.

- Seguridad Informática. Técnicas Criptográficas.
  Pino Caballero Gil.
  Edit. Ra – ma.

- Security In Computing.
  Charles P. Pfleeger.
  Edit. Prentice Hall.

- Seguridad e Integridad de Datos.
  Marc Farley, tom Stearns, Jeffrey Hsu.
  Edit. Mc Graw Hill.

- Secure Communications, Applications and Management.
  Roger J. Sutton.
  Edit. John Wiley and sons, LTD.

- Implementación de Redes Privadas Virtuales (RPV)
  Steven Brown
  Edit. McGraw Hill.

- Los Secretos de la Seguridad en Internet.
  John Vacca
  Edit. Anaya-Multimedia.

- Tarjetas Inteligentes.
  Juan Domingo Sandoval, Ricardo Brito, Juan Carlos Mayor.
  Edit. Paraninfo.

- Virtual Private Networks.
  Charlie Scott, Paul Wolfe y Mike Eerwin.
  Edit. O'Reilly

- Internet Security.
  Bradley Dunsmore, Jeffrey W. Brown, Michael Cross.
  Edit. Syngress.

Sitios en la red de Internet.

- www.csc.vill.edu
- www.geocities.com/articulos/seguridad.htm
- www.enterprisesecurity.com
- www.creat-tech.com
- www.seguridadenlared.org
- www.bankhacker.com
- http://mx.geocities.com/fundamentosdeseguridad/seminario/TEMA_7.htm
- http://spisa.act.uji.es/~mario/pem.html-multiple/partes.htm
- www.microsoft.com
- www.geocities.com/erichernandezp/protocolos_vpn.htm