Unidad VII: Conceptos de Seguridad

Introducción

La infraestructura de red, los servicios y los datos contenidos en las computadoras conectadas a la red son activos comerciales y personales muy importantes. Comprometer la integridad de estos activos puede ocasionar serias repercusiones financieras y comerciales.

Algunas de las consecuencias de la ruptura en la seguridad de la red son:

- interrupciones de red que impiden la realización de comunicaciones y de transacciones, con la consecuente pérdida de negocios,
- mal direccionamiento y pérdida de fondos personales o comerciales,
- propiedad intelectual de la empresa (ideas de investigación, patentes o diseños) que son robados y utilizados por la competencia, o detalles de contratos con clientes que se divulgan a los competidores o son hechos públicos, generando una pérdida de confianza del mercado de la industria.

Existen dos tipos de cuestiones de seguridad de la red que se deben tratar a fin de evitar serias consecuencias: *seguridad de la infraestructura de la red y seguridad del contenido.*

Asegurar la infraestructura de la red incluye la protección física de los dispositivos que proporcionan conectividad de red y evitan el acceso no autorizado al software de administración que reside en ellos.

La seguridad del contenido se refiere a la protección de la información contenida en los paquetes que se transmiten en la red y la información almacenada en los dispositivos conectados a ésta. Al transmitir la información en Internet u otra red, los dispositivos y las instalaciones por las que viajan los paquetes desconocen el contenido de los paquetes individuales. Se deben implementar herramientas para proporcionar seguridad al contenido de los mensajes individuales sobre los protocolos subyacentes que rigen la forma en que los paquetes se formatean, direccionan y envían. Debido a que el reensamblaje y la interpretación del contenido se delegan a programas que se ejecutan en sistemas individuales de origen y destino, muchos de los protocolos y herramientas de seguridad deben implementarse también en esos sistemas.

Las medidas de seguridad que se deben tomar en una red son:

- Evitar la divulgación no autorizada o el robo de información,
- Evitar la modificación no autorizada de información, y
- Evitar la Denegación de servicio.

Redes Seguras y Políticas

Una red segura debe ser capaz de:

- Garantizar la confidencialidad,
- Mantener la integridad de la comunicación, y
- Garantizar la disponibilidad.

Garantizar la confidencialidad

La privacidad de los datos se logra permitiendo que lean los datos solamente los receptores autorizados y designados (individuos, procesos o dispositivos).

Un sistema seguro de autenticación de usuarios, el cumplimiento de las contraseñas difíciles de adivinar y el requerimiento a los usuarios para que las cambien frecuentemente ayudan a restringir el acceso a las comunicaciones y a los datos almacenados en los dispositivos adjuntos de la red. Cuando corresponda, el contenido encriptado asegura la confidencialidad y reduce las posibilidades de divulgación no autorizada o robo de información.

Mantener la integridad de las comunicaciones

La integración de datos significa que la información no se alteró durante la transmisión de origen a destino. La integración de datos puede verse comprometida cuando al dañarse la información, ya sea en forma intencional o accidental, antes de que el receptor correspondiente la reciba.

La integridad de origen es la confirmación de que se validó la identidad del emisor. Se compromete la integridad del origen cuando un usuario o dispositivo falsifica su identidad y proporciona información incorrecta al destinatario.

El uso de firmas digitales, algoritmos de hash y mecanismos de checksum son formas de proporcionar integridad de origen y de datos a través de la red para evitar la modificación no autorizada de información

Garantizar disponibilidad

La garantía de confidencialidad e integridad son irrelevantes si los recursos de red están sobrecargados o no disponibles. Disponibilidad significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados. Los recursos pueden no estar disponibles durante un ataque de Denegación de servicio (DoS) o por la propagación de un virus de computadora. Los dispositivos firewall de red, junto con el software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y solidez del sistema para detectar, repeler y resolver esos ataques. La creación de infraestructuras de red completamente redundantes, con pocos puntos de error, puede reducir el impacto de esas amenazas.

Por que no hay una definición absoluta de lo que es una red segura, el primer paso que debe tomar una organización para lograr un sistema seguro, es definir la política de seguridad, la cual no especifica la forma de lograr la protección, pero si dice claramente y sin ambigüedades cuales son los elementos que deben ser protegidos.

Las políticas de seguridad son complejas porque implican la conducta humana, así como equipo e instalaciones de red. Una política de seguridad no se puede definir a menos que una organización entiende el valor de su información, en muchos casos el valor de la información es difícil de evaluar.

Consideremos, por ejemplo, una base de datos de nómina simple que contiene un registro para cada empleado, las horas que el empleado trabajo y el tipo de salario. Si algunos empleados fueron capaces de acceder a la información, pueden algunos empleados estar molestos y demandar salarios más altos o amenazar con irse, si los competidores obtuvieron la información pueden utilizarla para atraer a los empleados, también un competidor podría ser capaz de utilizar la información de forma inesperada (por ejemplo, para evaluar el esfuerzo invertido en un proyecto en particular).

Una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad. Las políticas de seguridad deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cubre el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Aspectos de la seguridad

Definir una política de seguridad también es complicado porque cada organización debe decidir qué aspectos de la protección son los más importantes, esto establece un compromiso entre la seguridad y la facilidad de uso.

Para ser capaz de entender los tipos de amenazas a la seguridad que existen, conviene definir los requisitos en seguridad. La seguridad en computadoras y redes implica tres requisitos:

- *Secreto:* requiere que la información en un computador sea accesible para lectura solo por los entes autorizados.
- *Integridad:* requiere que los recursos de un computador sean modificados solamente por entes autorizados. La modificación incluye escribir, cambiar, cambiar de estado, suprimir y crear.
- *Disponibilidad:* requiere que los recursos de un computador estén disponibles a los entes autorizados.

Una clasificación útil de las agresiones a la seguridad en red se hace en términos de agresiones pasivas y agresiones activas.

Agresiones pasivas: son del tipo de las escuchas, o monitorizaciones de las transmisiones. La meta del oponente es obtener información que está siendo transmitida. Existen dos tipos de agresiones pasivas, la divulgación del contenido de un mensaje y el análisis del tráfico.

Los ataques pasivos son muy difíciles de detectar ya que no implican la alteración de los datos.

Agresiones activas: suponen alguna modificación del flujo de datos o la creación de flujos falsos y subdividen en 4 categorías:

- Enmascaramiento: tiene lugar cuando la entidad pretende ser otra diferente.
- Repetición: supone la captura pasiva de unidades de datos y su retransmisión subsecuente para producir un efecto no autorizado.
- Modificación de mensajes significa que alguna porción de un mensaje legitimo se altera o que el mensaje se retrasa o se reordena para producir un efecto no autorizado
- Denegación de un servicio previene o inhibe el uso o gestión normal de las facilidades de comunicación.

Las agresiones activas presentan características opuestas a las agresiones pasivas. Mientras una agresión pasiva es difícil de detectar, existen medidas disponibles para prevenirlas.

Responsabilidad y control

Una organización puede darse cuenta de que no es capaz de diseñar una política de seguridad, porque no ha especificado como la responsabilidad de la información es asignada o controlada.

- La responsabilidad se refiere a mantener un registro de auditoría. ¿Quién es responsable de cada artículo de información? ¿Cómo guardan ellos los registros de acceso y cambio?
- La autorización se refiere a la responsabilidad de cada elemento de información y como tal responsabilidad se delega a los demás. ¿Quién es responsable de donde la información reside? ¿Cómo hace una persona responsable para aprobar el acceso y el cambio?

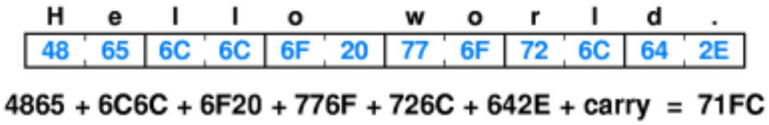
El tema crítico es el control. Una organización debe controlar el acceso a la información de la misma manera que controla el acceso a recursos físicos como oficinas, equipo, y provisiones.

Mecanismos de seguridad

Existen distintas técnicas que se emplean para asegurar la integridad *Bits de paridad:* Se emplea un bit de paridad para asegurar que cada carácter llega intacto. El emisor calcula un bit adicional que es un digito binario que indica si el número de bits con un

valor 1 en un conjunto de bits es par o impar y transmite esto como un octavo bit. El receptor realiza el mismo cómputo y verifica que los bits de paridad estén de acuerdo. El cálculo se hará de forma que una alteración de un bit pueda ser detectado.

Checksums o Sumas de comprobación: Muchas redes de ordenador envían una suma con cada paquete para ayudar al receptor a descubrir errores. Para calcular una suma, el emisor trata los datos como una secuencia de números enteros binarios y calcula su suma.



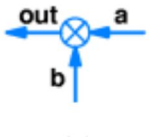
Cada par de caracteres se trata como un entero de 16 bits. Si la suma sobrepasa los 16 bits, el bit de carry se agrega al total. Las ventajas de las sumas de comprobación son el tamaño y la facilidad de cálculo. Además requiere muy poco cómputo y el costo de envío adicional de 16-bits es insignificante. Sin embargo, las sumas de comprobación no detectan todos los errores comunes, como se ilustra a continuación:

Data Item In Binary	Checksum Value	Data Item In Binary	Checksum Value
0001	1	0011	3
0010	2	0000	0
0011	3	0001	1
0001	1	0011	3
totals	7		7

Un error de transmisión ha invertido el segundo bit en cada uno de los cuatro elementos de datos, sin embargo las sumas de comprobación son idénticas.

CRCs Comprobaciones de Redundancias Cíclicas: Es posible detectar más errores sin aumentar la cantidad de información adicional en el paquete, usando la técnica CRC

(Comprobación de Redundancia Cíclica). El hardware necesario para generarlos es muy simple, los dos componentes necesarios son una OR exclusiva (o XOR) y un registro de desplazamiento.

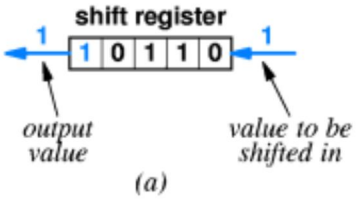


(a)

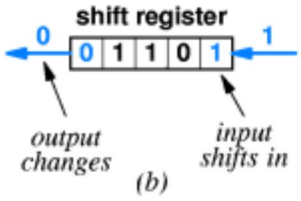
a	b	out
0	0	0
0	1	1
1	0	1
1	1	0

(b)

En (a), tenemos el diagrama para el hardware que calcula el XOR. En (b), tenemos el valor de salida para cada una de las cuatro combinaciones de valores de entrada. El segundo componente, un registro de desplazamiento, tiene un número fijo de bits y cada vez un nuevo bit entra (a la derecha) el contenido del registro se desplaza a la izquierda y el bit más a la izquierda se convierte en el valor de salida.



(a)



(b)

En (a) tenemos la posición antes del cambio y en (b) la posición después del cambio. El registro de desplazamiento puede ser inicializado mediante el establecimiento de todos los bits a cero.

Control de acceso y contraseñas

Las empresas, organizaciones y usuarios individuales gastan grandes cantidades de dinero en sistemas para su uso, tanto para el personal, los amigos o ellos mismos. Proteger la información de esa máquina puede ser importante y regular quien tenga

acceso a los sistemas, servicios y datos es una tarea necesaria, especialmente si estos sistemas puede acceder todo el mundo o incluso a una red de área local a través de una conexión de red.

Una forma común de proporcionar servicios básicos de seguridad es a través de la utilización de mecanismos de control de acceso, el más común es la protección mediante contraseñas. El uso de las contraseñas, aunque es muy rudimentario, actúa como clave para acceso al sistema. Los proveedores de sistemas deben ofrecer los mecanismos para evitar que los usuarios del sistema accedan a archivos que se les prohibió o ingresar a lugares donde no son bienvenidos.

Un mecanismo que puede ofrecer este modelo de seguridad es el de una matriz de acceso. Una matriz de acceso está compuesta de los elementos indicados por sujeto, objeto y el derecho de acceso. Estos elementos indican:

Sujeto: Quien puede acceder a un recurso (ya sea de usuario, procesos, etc)

Objeto: un recurso que puede ser accedido, como los segmentos de memoria o archivos.

Derecho de acceso: cómo el objeto puede ser accedido por un usuario o proceso en particular.

	Accounting Program	User DB file	Archive File
User1	Read/Execute		
Process X		Read/Write	
Process Y	Read	Read	Read/Write
User2		Read/Write	

La matriz puede ser descompuesta por fila o columna para obtener acceso a la información. Por ejemplo, si la matriz se descompone por columnas entonces lo que se obtiene es una lista de control de acceso de los derechos que se le da a cada usuario, grupo o procesos a acceder a ese objeto en particular. Por otra parte, si la matriz se

descompone en filas entonces lo que se obtiene es una lista que enumera todo lo que el usuario es capaz de acceder y qué derecho de acceso tiene.

Passwords

La mayoría de los usuarios de un sistema informático utiliza un sistema de identificación y contraseña para que se le conceda el acceso.

En general, el identificador de usuario (userid), a través de algún tipo de lista de control de acceso determinará los recursos que el usuario está autorizado a utilizar, la contraseña se utiliza para autenticar al usuario. Las contraseñas que identifican a los usuarios tienen que ser almacenados en algún lugar y esto proporciona una medida de la vulnerabilidad es por ello que generalmente la contraseña se cifra.

Cifrado e intimidad

Los mecanismos de protección, como el uso de contraseñas, muchas veces no son suficientes para mantener información confidencial adecuadamente resguardada. Con el uso masivo de las redes de computadores, más y más información se transmite por ella, y nadie puede estar seguro de que no haya personas dispuestas a acceder a la información que se transmite. Los métodos criptográficos son los más comúnmente usados para proteger información confidencial. Lo que se envía por la red no es la información original, sino la información codificada, que carece de sentido salvo para el receptor, que puede decodificarla.

La criptografía es la herramienta fundamental en la seguridad por que la encriptación puede garantizar la confidencialidad de los datos (algunas veces llamada privacidad), la autenticación de mensajes, la integridad de los datos y pueden evitar ataques. Se aplica un remitente de cifrado con los bits del mensaje de tal manera que sólo el destinatario puede descifrar. Alguien que intercepta una copia de un mensaje cifrado no será capaz de extraer información. Además, un mensaje cifrado puede incluir información como la longitud del mensaje que un atacante no puede truncar el mensaje sin ser descubierto

La terminología empleada con la encriptación se define por cuatro ítems:

- Texto Plano: mensaje original antes de ser cifrado
- Texto Cifrado: mensaje después de haber sido encriptado
- Clave de encriptación: un string usado para encriptar el mensaje
- Clave de desencriptacion: un string usado para desencriptar el mensaje

En algunas tecnologías, la clave de encriptación y desencriptación son idénticas y en otras son diferentes.

Matemáticamente, podemos considerar a la encriptación como una función, *encriptar*, que toma dos argumentos, K clave, y M el texto plano a cifrar. La función produce una versión encriptada del mensaje C

$$C = \textit{encriptar}\ (K_1, M)$$

La función de desencriptación funcionara de manera inversa produciendo el mensaje original

$$M = \text{desencriptar}\ (K_2, C)$$

Existen muchas tecnologías de encriptación, y pueden dividirse en dos categorías que se definen de acuerdo al uso de las claves:

- Clave privada
- Clave publica

En el cifrado de clave privada, cada par de las entidades que se comunican comparten una clave única que funciona como una clave de cifrado y una clave de descifrado. El nombre se debe a que la clave debe ser mantenida en secreto, si un tercero realiza una copia de la clave, el tercero será capaz de descifrar el paso de mensajes entre las entidades. El cifrado de clave privada es simétrico en el sentido que pueden enviar o recibir mensajes.

Para enviar un mensaje se utiliza la clave para producir el texto cifrado que luego se envía a través de la red.

Cuando llega un mensaje, el lado receptor utiliza la clave secreta para descifrar el texto cifrado y extraer el mensaje original. Así que en el cifrado de clave privada el emisor y el receptor utilizan la misma clave, K, lo que significa que:

$$M = \textit{desencriptar}\ (K, \textit{encriptar}\ (K, M))$$

Cifrado de Clave pública

El cifrado de clave pública encuentra su utilización en la autentificación de mensajes y la distribución de claves.

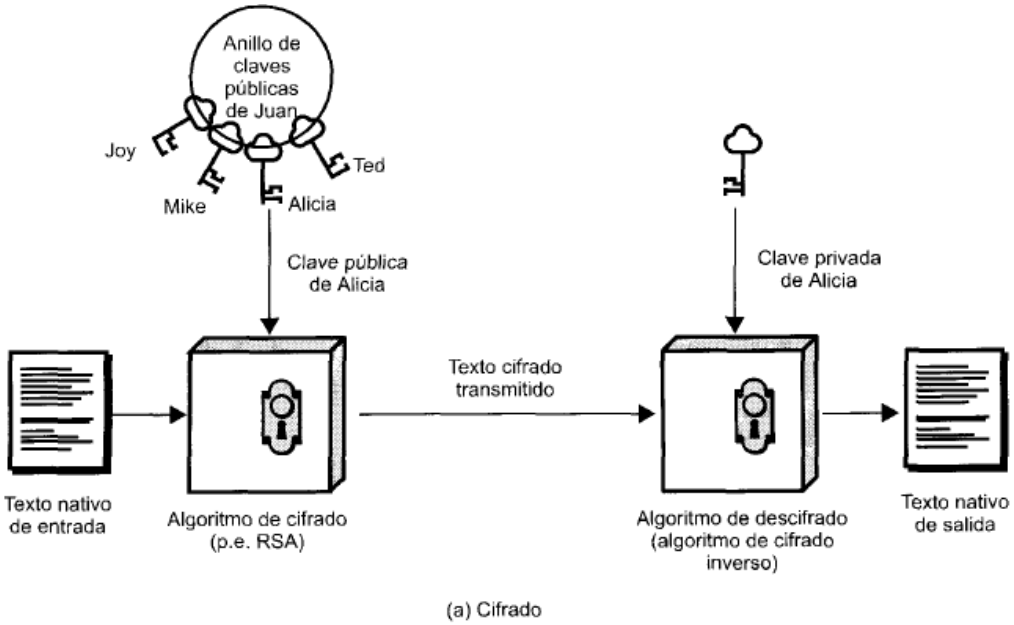
El algoritmo de clave pública se basa en funciones matemáticas en lugar de sustitución y permutaciones. Pero lo más importante, la criptografía de clave pública es asimétrica y

supone el uso de dos claves independientes, en contraste con el cifrado simétrico convencional, que solo utiliza una clave.

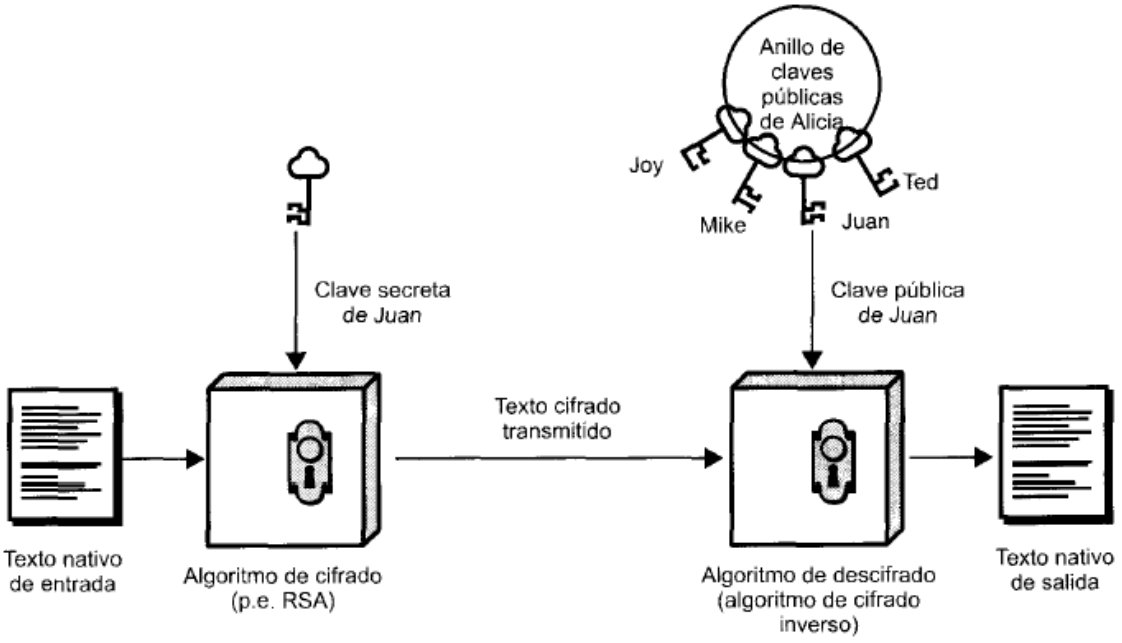
Utilizar dos claves tiene consecuencias profundas en las áreas de privacidad, distribución de claves y autentificación.

El esquema de cifrado de clave pública tiene:

- Texto nativo: es el mensaje legible o datos que se pasan al algoritmo como entrada.
- Algoritmo de cifrado: el algoritmo de cifrado lleva a cabo varias operaciones sobre el texto nativo.
- Clave pública y privada: este es el para 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 cifrado y la otra clave y produce el texto nativo original.



(a) Cifrado



(b) Autentificación

Como el nombre lo sugiere, la clave pública del par se hace pública 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 un clave de cifrado y en una clave diferente, pero relacionada, para el descifrado. Además, estos algoritmos tienen las siguientes características:

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 pública, cualquiera de las dos claves que se utilizan, se puede emplear para el cifrado y la otra para el descifrado.

Los pasos esenciales son los siguientes:

1. Cada usuario genera un para 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 público. Esta es la clave pública. La clave compañera se mantiene privada, cada usuario mantiene una colección de claves públicas de otros usuarios.

3. Por ejemplo, si Juan desea enviar un mensaje privado a Alicia, Juan cifra el mensaje utilizando la clave pública 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 su clave privada.

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 pública obsoleta.

Validación de identificación con firmas digitales

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 lo 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 más ha podido crear el texto cifrado que se descifra con la clave pública 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 autenticado en términos de la fuente y de integridad de los datos.

En el esquema precedente, se cifra el mensaje entero, lo que, aunque valida al autor y al contenido, requiere una gran cantidad de almacenamiento. Cada documento se debe guardar 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 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 no proporciona privacidad. Esto es, el mensaje que se envía está seguro frente a alteraciones, pero no lo está 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 está cifrado.

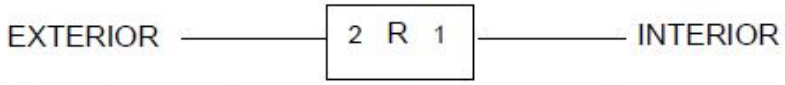
Incluso en el caso de cifrar el mensaje entero, no hay protección de confidencialidad y que cualquier observador puede descifrar el mensaje utilizando la clave pública del emisor.

Filtrado de paquetes

Muchos routers comerciales ofrecen un mecanismo que aumenta el ruteo normal y permite que el administrador tenga un mayor control en el procesamiento de paquetes. Informalmente conocidos como FILTROS DE PAQUETES el mecanismo requiere que el administrador especifique como deberá manejar el ruteador coda datagrama. Por ejemplo, el administrador podría elegir para filtrar todos los datagramas que provengan de una fuente en particular o los utilizados para una aplicación particular mientras selecciona la ruta para otros datagramas.

El termino filtrado de paquetes se debe a que el mecanismo de filtrado no conserva un registro de las interacciones o una historia de los datagramas previos. Por el contrario, el filtro considera a cada datagrama de manera separada. Cuando un datagrama llega primero, el ruteador pasa el datagrama a través de su filtrado de paquetes antes de realizar cualquier otro procesamiento. Si el filtro rechaza el datagrama, el ruteador lo desecha de inmediato.

Dado que el TCP/IP no dicta un estándar para el filtrado de paquetes. Cada vendedor de ruteadores es libre de seleccionar las características de su filtro de paquetes así como la interfaz que un administrador utiliza para configurar el filtro. Algunos ruteadores permiten al administrador configurar acciones de filtrado separadas para cada interfaz, mientras que otros tiene una sola configuración para todas las interfaces. Por lo general, cuando se especifican datagramas que el filtro debe bloquear, un administrador puede listar cualquier combinación de direcciones IP fuentes, direcciones IP destino, protocolos, numero de puerto de protocolo fuente y numero de puerto de protocolo destino.



Llegadas a la interfaz	Fuente IP	Destino IP	Protocolo	Puerto fuente	Puerto Destino
2	*	*	TCP	*	21
2	*	*	TCP	*	23
1	128.5.*.*	*	TCP	*	25
2	*	*	UDP	*	43
2	*	*	UDP	*	69
2	*	*	TCP	*	79

Ruteador con dos interfaces y un ejemplo de especificación de filtro de datagramas.

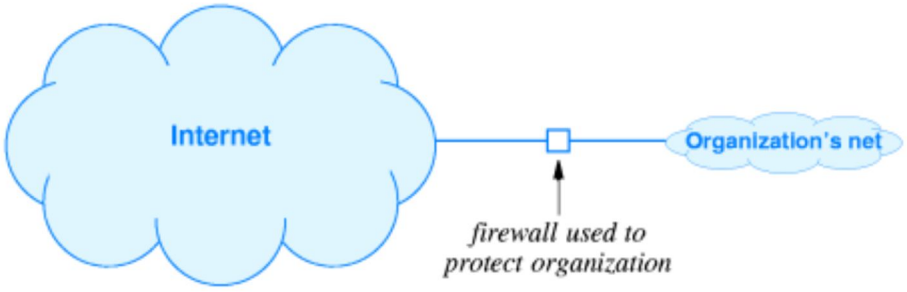
En el ejemplo el administrador ha elegido, bloquear datagramas destinados a unos cuantos servicios bien conocidos y bloquear un caso de datagramas que salen. El filtro bloquea todos los datagramas que salen y que se originan desde cualquier anfitrión en la red de clase B 128.5.0.0

Esta destinado a un servidor de correo electrónico remoto (TCP puerto 25). El filtro también bloquea datagramas entrantes destinados a FTP (TCP puerto 21) TELNET (TCP puerto 23), WHOIS (UDP puerto 43), TFTP (Puerto 69) o FINGER (TCP puerto 79).

Concepto de Internet Firewall

Aunque la tecnología de cifrado ayuda a resolver muchos problemas de seguridad, una segunda tecnología es necesaria. Esta tecnología es conocida como un firewall de Internet, la cual ayuda a proteger a los equipos de una organización y redes del tráfico de Internet no deseado. Al igual que un firewall convencional, un firewall de Internet está diseñado para evitar que los problemas de Internet se extiendan a los ordenadores de la organización .

Un firewall se coloca entre una organización y el resto de Internet, y todos los paquetes de entrada o salida de la organización pase por el firewall.



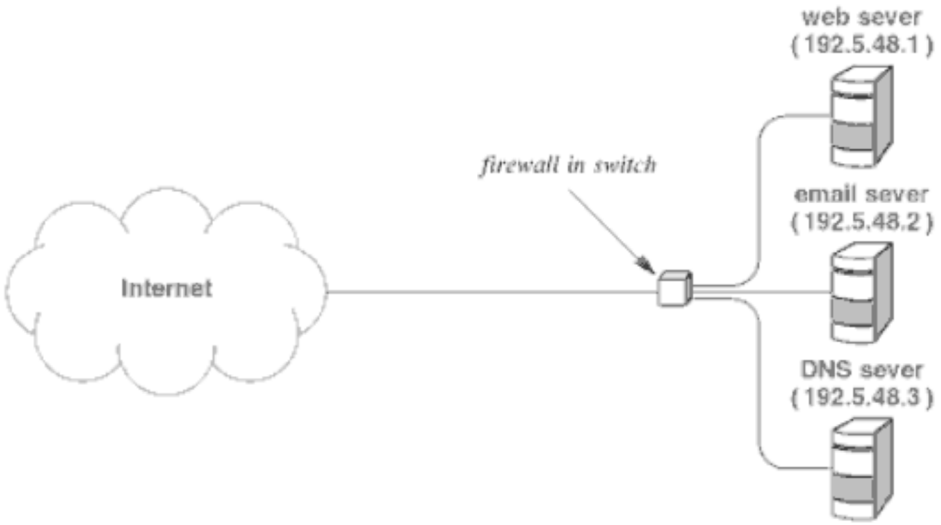
Si una organización tiene varias conexiones a Internet, un firewall debe colocarse en cada una, y todos los firewalls de la organización deben estar configurados para hacer cumplir la política de seguridad de la organización.

Además, el propio firewall debe ser protegido contra la manipulación indebida. En resumen:

- Todo el tráfico que llega a la organización pasa a través de un firewall
- Todo el tráfico que deja pasar la organización, pasa a través de un firewall
- El firewall implementa la política de seguridad y descarta paquetes que no se adhieren a la política
- El propio firewall es inmune a los ataques a la seguridad

Los firewalls son la herramienta de seguridad más importante utilizados para manejar la conexión entre dos organizaciones que no confían entre sí. Al colocar un firewall en cada conexión de red externa, la organización puede definir un perímetro de seguridad que impide que los intrusos puedan interferir en las computadoras de la organización.

Un firewall, utiliza el filtrado de paquetes para impedir la comunicación de paquetes no deseados. Cada especificación de filtro da una combinación de campos de cabecera, incluyendo direcciones IP de origen y destino, números de puerto, así como el tipo de protocolo de transporte.



Dir	FRAME TYPE	IP SOURCE	IP DEST	IP TYPE	SRC PORT	DST PORT
in	0800	*	192.5.48.1	TCP	*	80
in	0800	*	192.5.48.2	TCP	*	25
in	0800	*	192.5.48.3	TCP	*	53
in	0800	*	192.5.48.3	UDP	*	53
out	0800	192.5.48.1	*	TCP	80	*
out	0800	192.5.48.2	*	TCP	25	*
out	0800	192.5.48.3	*	TCP	53	*
out	0800	192.5.48.3	*	UDP	53	*

Ejemplo de configuración de firewall para un sitio con tres servidores, el asterisco se utiliza para denotar una entrada comodín que coincide con cualquier valor.