Aspectos de Seguridad en Redes

Introducción

En la actualidad la seguridad informática juega un papel preponderante en las comunicaciones entre distintos ordenadores, debido a la cantidad de plataformas disponibles y a las condiciones las cuales cambian de manera rápida. La posibilidad de interconectarse a través de distintas redes ha abierto un universo nuevo de posibilidades, trayendo consigo la aparición de nuevas amenazas a los sistemas computarizados.

En este aspecto es importante establecer cuál es la importancia que representan los datos, como se están enviando y que vulnerabilidades pueden presentar estos cuando son enviados a través de una red de comunicaciones. En este capítulo se analizaran cuales son estos ataques y cuales medidas pueden ser implementadas para tratar de minimizar al máximo el riesgo de la intercepción o captura de datos en las conexiones de redes.

Pero antes de eso deberíamos definir que es la seguridad en redes, la cual de acuerdo a los elementos que conocemos y los aspectos que acabamos de mencionar podemos decir que la seguridad en redes es mantener bajo protección los recursos y la in formación con que cuenta la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de la información.

Uno de los mayores obstáculos para que la redes pudieran desarrollarse era el de encontrar lenguajes comunes para que las computadoras de diversos tipos pudieran comunicarse, aquí es donde TCP/IP se ha instaurado como el modelo a seguir por todos. Uno de los mayores obstáculos que han tenido que superarse para que las redes pudieran desarrollarse, ha sido encontrar lenguajes comunes para que computadoras de diferentes tipos pudieran entenderse. En este sentido el protocolo TCP/IP se ha erigido como estándar de facto, aunque por supuesto el análisis realizado dependerá del tipo de red con el cual se esté trabajando, debido a que los riesgos serán distintos, los cuales conducirán a medidas totalmente diferentes para evitar y defender a los sistemas de esos riesgos. En este sentido antes de ahondar en el capitulo haremos una breve descripción de los diversos tipos de redes y las amenazas que podemos encontrar además de cómo poder sortearlas.

Redes Internas

El caso más sencillo que se puede encontrar, el de una red local (LAN): un grupo de computadores conectados a través de un medio físico (cables) de los cuales se tiene acceso total. En este tipo de redes es posible ejercer un control sobre el canal de comunicaciones, pudiendo protegerlo para evitar posibles pérdidas de información. Uno de los riesgos existentes en este tipo de redes es la

perdida de información debido a fallos físicos, los cuales pueden ser minimizados llevando a cabo una política de respaldo de información adecuada.

Debido a que un control total sobre el medio físico es imposible se presenta otro de los riesgos en redes LAN, el de la suplantación de un computador; por ejemplo una red LAN presente en alguna oficina, o inclusive algún recinto educativo, donde hay un conjunto de computadores conectados vía Ethernet, seria (si el acceso no es muy restringido) relativamente sencillo para una persona conectar un computador portátil y realizar algún análisis de tráfico, intentar acceder a los demás equipos e incluso difundir algún tipo de código malicioso a través de toda la red. En este caso las estrategias a tomar son: deshabilitación dinámica de las conexiones no utilizadas en algún momento, control de dirección MAC de cada equipo (aunque no muy seguro debido a la posibilidad de poder, si se conocen las direcciones permitidas, suplantar cualquier dirección MAC) o utilizar algún protocolo de autenticación de computadoras dentro de una red.

Redes Externas

Una red externa es aquella en la que su comunicación se basa total o parcialmente sobre un canal sobre el cual no se tiene ningún tipo de control (ejemplo: una red LAN conectada a Internet). Para identificar los posibles riesgos que pueden afectar a estas redes se deben chequear diversos aspectos como: sistema operativo de los computadores conectados a la red, o los diversos tipos de acceso que cada usuario tiene sobre la comunicación.

Una de las configuraciones más utilizadas para proteger estas redes es el uso de una red local conectada al exterior a través de un firewall (equipo que filtra el tráfico entre la red interna y la externa). Pero existen diversas configuraciones de firewall, en la fig. 1 vemos dos tipos, la primera mas económica pero también más vulnerable ya que no evita que se pueda acceder a la red interna, y la segunda mas recomendada, donde hay una total separación entre las redes.

Insertar Fig. 1

Existen dos grandes peligros potenciales que pueden comprometer este tipo de redes:

Ataques Indiscriminados: son los más comunes, y también los menos dañinos, dentro de esta categoría entran los códigos maliciosos como virus, malwares, etc., los cuales no son más que códigos de programación diseñados para introducirse en los sistemas y producir en ellos diversos efectos. Debido a su carácter general existen maneras muy comunes de defenderse como antivirus, antispyware, etc.

Ataques a medida: son menos comunes y mucho más dañinos, en este caso el ataque esta centralizado y focalizado hacia algún punto en particular, por lo que las medidas para defenderse del mismo no son eficientes ya que el ataque puede ser de cualquier forma.

Aspectos sobre la seguridad de la información

La seguridad de la información se puede clasificar en tres aspectos importantes:

- ✓ Seguridad de las computadoras
- ✓ Seguridad de la Red (Intranet)
- ✓ Seguridad de Redes Interconectadas (Internet)

No existe una frontera clara entre estos tres aspectos, debido a lo interrelacionados que están entre sí. La seguridad de las redes de computadoras se puede organizar en tres aspectos, a saber:

Servicios de Seguridad

Un adecuado plan de seguridad debe comprender ciertos elementos necesarios para asegurar que el plan funcione de manera correctamente. Estos elementos comprenden una arquitectura basada en criptografía la cual se muestra en la fig. 2 y se detalla a continuación:

Insertar fig.2

Autenticación: es el proceso de verificar a los usuarios antes de dejarlos entrar en el sistema, esto se realiza comparando la información recibida con aquella almacenada en una base de datos. En este caso existen dos tipos de autenticación:

a. Autenticación de un mensaje único: en este caso su función es indicarle al receptor que el mensaje proviene realmente de la fuente de donde dice provenir
b. Autenticación de una comunicación: cuando se establece una comunicación entre un dos equipos se deben tomar en cuenta dos partes: la primera donde se autentican ambos usuarios determinando que cada quien es quien dice ser, y una segunda en donde el servicio debe asegurar la conexión de manera que impida que algún tercero quiera (enmascarado como alguno de los dos usuarios) irrumpir en la comunicación intentando transmitir o recibir información sin autorización.

Control de Acceso: la función es interrumpir el acceso no autorizado a cualquier recurso, esto quiere decir que no tiene permisos para usar, modificar o eliminar algún recurso. Para lograr este control cada unidad deberá primero autenticarse para determinar si posee o no los privilegios para la actividad que desea realizar.

Confidencialidad e Integridad: la confidencialidad se refiere a asegurar que la información no sea revelada a personas no autorizadas, y se proteja contra ataques pasivos, la intercepción de datos por ejemplo, esto garantiza que los datos no hayan sido alterados interna o externamente en el sistema.

La integridad se refiere a que los datos sean transmitidos sin sufrir ningún tipo de modificación, alteración, borrado, duplicación, etc. Realizadas por personas sin autorización

No Repudiación: es el proceso mediante el cual se obtiene una prueba irrefutable de que ambas partes son quienes dicen ser, de manera que ninguna pueda negar la comunicación.

Técnicas de Encriptación: básicamente se refiere a ciertos mecanismos que van a permitir mantener la confidencialidad de los datos, dentro de esto se encuentra la criptografía y las firmas digitales, que no es más que el proceso de "cifrar" la información para que solo sea entendible para los elementos con el acceso adecuado, requiere de un algoritmo de encriptación y un esquema de administración de claves. Más adelante estaremos ahondando un poco más en este tema.

Ataques a la Seguridad:

Existen diversos tipos de ataques que se pueden realizar a un sistema de comunicaciones, y dependiendo del tipo dependerá también la respuesta que se pueda plantear ante estos. En este apartado se ahondara un poco sobre este asunto.

Si los ataques se encuentran dirigidos directamente hacia los datos que se están comunicando pueden entrar dentro de las siguientes categorías:

Interrupción: esto se refiere cuando se interrumpe totalmente el flujo normal de las comunicaciones, debido a que una parte o todo el sistema no pueden utilizarse. Ejemplo: destrucción física de equipos, borrado de aplicaciones, falla de sistema operativo, etc.

Intercepción: esto se refiere a cuando hay algún acceso no autorizado al sistema, por parte de una persona, software o sistema de comunicación y debido a que no se pierden datos es uno de los ataques más difíciles de interceptar. Ejemplo: reproducción ilícita de archivos, intercepción de los cables para monitoreo de datos en una red, etc.

Modificación: acceso no autorizado al sistema además de la modificación del mismo. Ejemplo: modificaciones de bases de datos, cambios en la configuraciones de software del sistema, etc.

Fabricación: acceso autorizado al sistema además de la adición de objetos que previamente no estaban. Ejemplo: insertar registros en bases de datos, añadir transacciones a un sistema de comunicaciones, etc.

Ins img 3

Ahora pasaremos a dar una explicación un poco más amplia de los ataques, muchas de estas amenazas se enfocan en lo que conocemos como Negación del Servicio (Denial of Service, o DoS en ingles), en este tipo de ataques la meta fundamental es negar al equipo bajo ataque el acceso a un recurso determinado o a sus propios recursos, algunos ejemplos de este tipo de ataques son:

- Tentativas de inundar una red, evitando de esta manera el tráfico Legítimo de datos en la misma;

- Tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio;
- Tentativas de evitar que una determinada persona tenga acceso a un servicio;
- Tentativas de interrumpir un servicio específico a un sistema o a un usuario;

Cabría tener en cuenta que, el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Por ejemplo, un "hacker" puede utilizar un área del FTP anónimo como lugar para salvar archivos, consumiendo, de esta manera, espacio en el disco y generando tráfico en la red.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar inoperativa una computadora o una red. De esta forma, toda una organización puede quedar fuera de Internet durante un tiempo determinado.

Modos de Ataque

Existen tres tipos de ataques de negación de servicios:

a. Consumo de recursos escasos, limitados, o no renovables: las computadoras y las redes necesitan para funcionar ciertos recursos: ancho de banda de la red, espacio de memoria y disco, tiempo de CPU, estructuras de datos, acceso otras computadoras y redes, entre otros. Los ataques de Negación de servicio se ejecutan, con frecuencia, contra la conectividad de la red. Otro de los ataques consiste en el consumo del ancho de banda de la red, generando una gran cantidad de paquetes dirigidos a la misma impidiendo así el uso de dicha red. Todo este tipo de ataque se basa en códigos que generan por así decirlo ruido en el sistema, por ejemplo si lo que se consume es espacio en memoria el ataque se basa en un programa que se "reproduce", es decir crea infinitas copias de sí mismo con lo que satura la memoria del equipo.
b. Destrucción o alteración de la información de configuración: este tipo de ataques se basa en que un equipo incorrectamente configurado puede no funcionar bien o directamente no arrancar.
c. Destrucción o alteración física de los componentes de la red: Es muy importante la seguridad física de la red. Se debe resguardar contra el acceso no autorizado a las computadoras, los routers, los racks de cableado de red, los segmentos del backbone de la red, y cualquier otro componente crítico de la red.

Prevención y Respuesta

Tal como se ha expresado anteriormente, los ataques de Negación de servicio pueden dar lugar a pérdidas significativas de tiempo y dinero para muchas organizaciones, por lo que se recomiendan una serie de medidas:

• Coloque access lists en los routers. Esto reducirá su exposición a ciertos ataques de negación de servicio

• Instale patches a su sistema operativo contra flooding de TCP SYN. Esta acción permitirá reducir sustancialmente su exposición a estos ataques aunque no pueda eliminar el riesgo en forma definitiva.

• Invalide cualquier servicio de red innecesario o no utilizado. Esto puede limitar la capacidad de un hacker de aprovecharse de esos servicios para ejecutar un ataque de negación de servicio. Por ejemplo: chargen, Echo, etc.

•Si su sistema operativo lo permite, implemente sistemas de cuotas. Por ejemplo, si su sistema operativo soporta "disk Quotas" impleméntelo para todos los logins. Si su sistema operativo soporta partición o volúmenes, separe lo crítico de lo que no lo es.

• Observe el funcionamiento del sistema y establezca valores base para la actividad ordinaria. Utilice estos valores para calibrar niveles inusuales de la actividad del disco, del uso de la CPU, o del tráfico de red.

Incluya como parte de su rutina, el examen de su seguridad física. Considere, entre otras cosas, los servidores, routers, terminales desatendidas, ports de acceso de red y los gabinetes de cableado.

•Utilice Tripwire o una herramienta similar para detectar cambios en la información de configuración u otros archivos.

• Trate de utilizar configuraciones de red redundantes y fault-tolerant.

Técnicas de Encriptación

La encriptación es un método para transformar un texto plano a texto cifrado, con la posibilidad de recuperar luego el texto plano a partir del texto cifrado. Se puede emplear la encriptación en un equipo de red a través de una Red Privada Virtual (Virtual Private Network –VPN). Una VPN brinda conexiones seguras entre puntos donde la información encriptada puede viajar en una red pública como Internet. Este proceso de transformación / recuperación se lleva a cabo siguiendo un procedimiento preestablecido conocido como algoritmo de encriptación, que depende principalmente de un parámetro denominado clave o clave secreta. En la Figura 4 se presenta un esquema del proceso de encriptación.

a) La información original (texto plano) es procesada por un algoritmo de encriptación, que utiliza una clave de encriptación para cifrar el texto.

b) El resultado de dicho proceso se denomina texto cifrado.

c) El receptor recibe el texto cifrado y lo desencripta mediante una clave secreta para obtener el mensaje original.

Ins Fig. 4

Clasificación de los sistemas criptográfico

Todos los algoritmos de encriptación se basan en dos principios generales: sustitución y transposición.

a. Técnicas de Sustitución

En estas técnicas cada elemento del texto plano (bit, letra, grupo de bits o letras) se mapea en otro elemento. Estos cifradores utilizan una palabra o número clave. La primera letra del mensaje se puede cifrar añadiéndole el valor numérico de la primera letra de la palabra clave; la segunda se cifra de forma análoga, utilizando la segunda letra de la palabra clave, y así sucesivamente, repitiendo la palabra clave tantas veces como sea necesario para cifrar todo el mensaje. El sistema de tablas de Vigenère descansa en este principio.

b. Técnicas de transposición

En estas técnicas se reordenan los elementos del texto plano. Se logra un mapeo distinto con algún tipo de permutación del texto plano. La técnica más simple es la "cerca del riel" (rail fence), en que el texto plano se escribe en una secuencia de columnas y se lee como una secuencia de filas.

Número de claves utilizado

Si el transmisor y el receptor usan la misma clave, el sistema se llama simétrico, de una sola clave, de clave secreta, o encriptación convencional. Si el transmisor y el receptor usan claves distintas, el sistema es asimétrico, de 2 claves o encriptación de clave pública.

Métodos de encriptación

Los métodos de encriptación más usados son: encriptación simétrica y encriptación asimétrica.

a. Encriptación simétrica

Es aquélla donde la misma clave –que debe mantenerse en secreto– sirve para encriptar y desencriptar la información. Llamada encriptación clásica, convencional o de una sola clave, se usa básicamente al requerir una performance rápida de encriptación. Para fortalecer la seguridad la clave de sesión debe cambiarse con la mayor frecuencia posible. La figura 24.4 ilustra este método.

El procedimiento de encriptación simétrica es el siguiente: El mensaje en texto plano se encripta utilizando la clave compartida. El paquete encriptado pasa a través de la red

insegura. En el receptor, la misma clave compartida se emplea para desencriptar el texto cifrado y poder recuperar el texto plano.

Aunque la encriptación simétrica sólo utiliza una clave compartida, debemos tener en consideración los siguientes detalles antes de implementar este tipo de encriptación.

- ƒ Las claves deben permanecer secretas.
- ƒ Las claves deben cambiarse periódicamente.
- ƒ En grandes ambientes, generar, distribuir y proteger las claves resulta una labor compleja.

Un método común de encriptación simétrica es el que se realiza por medio de la Norma de Encriptación de Datos (Data Encryption Standard –DES).

Ins Im 5

b. Encriptación asimétrica

Este método también es conocido como encriptación de clave pública, debido a que el esquema de encriptación usa dos claves: una privada y una pública.

Img 6

Claves públicas según diffie-hellman

Estas claves se originan mediante el esquema de claves Diffie–Hellman, donde la clave pública de un servidor y la clave privada de otro servidor crean una clave secreta compartida, siendo matemáticamente casi imposible derivar la clave privada a partir de la clave pública. Esta clave secreta compartida se utiliza para verificar y desencriptar el paquete cifrado.

Firmas digitales

Las firmas digitales son una aplicación de las claves públicas. Las describimos a continuación. El protocolo básico de una firma digital (ver fig. 7) es el siguiente:

Ins img 7

Alicia encripta un documento con su clave privada, con lo cual está firmando implícitamente el documento. Alicia envía el documento firmado a Pedro. Pedro desencripta el documento con la clave pública de Alicia. Así, obtiene el documento original y además verifica la firma de Alicia, pues pudo abrir el documento con la clave pública de ella.

Conceptos de autenticación

Es el proceso de verificar la identidad del usuario antes permitirle ingresar al sistema, confrontando la información recibida con aquélla almacenada en una base de datos. En estos casos el usuario recibe el nombre de principal, término referido al legítimo poseedor de una identidad. En la

presente sección desarrollaremos el servicio de autenticación, para ello se explicarán los conceptos básicos, los passwords o contraseñas y los protocolos usados para el proceso de autenticación.

Definiciones y conceptos básicos de autenticación

La Autenticación se refiere al servicio mediante el cual se garantiza que una de las partes llamada el solicitante (claimant), que tiene la identidad de principal, solicita la autenticación de ésta y permite a otra parte llamada el verificador (verifier) declarar que la solicitud es legítima.

El servicio de autenticación se basa en alguno de los siguientes métodos:

ƒ El solicitante demuestra el conocimiento de algo, por ejemplo: un password.

ƒ El solicitante demuestra poseer algo, por ejemplo: una tarjeta.

ƒ El solicitante presenta una característica inmutable, por ejemplo: una huella digital.

ƒ Una evidencia de que el solicitante está en un lugar determinado en un momento determinado.

ƒ El verificador acepta la autenticación realizada por terceros.

Usar sólo uno de los métodos citados no brinda una completa seguridad sobre la identidad del usuario. Por eso se suelen combinar dos o más de ellos. Esta combinación se llama autenticación fuerte (Strong Authentication) y la usan la mayoría de productos comerciales de autenticación. La autenticación puede ser unilateral o mutua. La primera se da cuando sólo una de las partes autentica a la otra; la segunda, implica que cada una de las partes autentica a la otra.

Passwords o contraseñas

Los passwords, contraseñas o PIN (Personal Identification Number) constituyen parte de la mayoría de los sistemas de autenticación y se clasifican en dos tipos:

a) Passwords Estáticos

Son cadenas de letras o números usados en varias oportunidades para acceder a un sistema.

b) Passwords Dinámicos

Son cadenas de letras o números usados para acceder a un sistema, pero que siempre cambian.

Consideraciones sobre los passwords

Respecto a los passwords, se tiene que tener en cuenta los siguientes aspectos:

a) Debilidades de los Sistemas basados en passwords

Cada tipo de password tiene sus debilidades. Los passwords estáticos ya está alcanzando el fin de su ciclo de vida en los procesos críticos de autenticación, mientras que los sistemas basados en passwords dinámicos aún necesitan de mayor desarrollo y control. Los sistemas basados en passwords estáticos son vulnerables a muchas formas de ataque.

b) Ingeniería Social

Consiste en manipular a las personas para obtener sus contraseñas. Esto se puede lograr mediante una llamada telefónica, en la que se simula ser el administrador de la red o alguien vinculado al sistema solicitándole, con cualquier excusa, que le proporcione su password. También se considera en este grupo al hecho de observar qué teclas presiona el usuario al ingresar su password.

c) Almacenaje indebido

Estas técnicas pueden incluir el hecho de que el usuario anote o grabe su password en algún lugar de fácil acceso con la intención de recuperarlo después en caso de olvido.

d) Ataques por fuerza bruta

Una vez que el atacante logra acceder a la línea de comandos, copia el archivo encriptado de los passwords y mediante un programa “crack, program” descubre el password del usuario. El programa toma un archivo de texto y le aplica un algoritmo de encriptación, obteniendo un nuevo archivo encriptado. Luego compara el archivo obtenido y el copiado del sistema para hallar el password deseado. Una forma alternativa de ataque es adivinar el password del usuario considerando cadenas sencillas de caracteres, como el nombre o iniciales del usuario, su fecha de nacimiento, etc. Estos primeros tipos de ataques se suelen clasificar como debilidades externas del sistema.

e) Monitorización del teclado

La monitorización del teclado se puede hacer de varias formas. Una de ellas es ejecutar un programa que registre las teclas pulsadas y las guarde en un archivo para estudiarlo luego. Un método alterno puede ser, cuando no hay acceso físico al sistema, monitorizar las emisiones de la pantalla.

f) Monitorización de la red y ataques por medio de accesos grabados

La monitorización de la red o “sniffing” es el método más crítico relacionado con los passwords estáticos. Si se transmite el password sin protegerlo, será fácil para el atacante suplantar al legítimo usuario, empleando grabaciones de accesos válidos.

Control de acceso

La autorización concede derecho a un usuario para acceder a un recurso. El control de acceso es el medio de hacer cumplir esas autorizaciones. En general, se puede afirmar que el control de acceso es el método empleado para prevenir el uso no autorizado de los recursos.

Existen dos métodos para prevenir los accesos no autorizados:

a) Filtro de las solicitudes de acceso

Verifica los derechos de un usuario respecto a un recurso, cuando el usuario intenta acceder a éste.

b) Separación

Evita cualquier intento de acceso por parte de los usuarios no autorizados. El primer método se relaciona con los mecanismos de control de acceso, que detallaremos más adelante; el segundo implica medidas como seguridad física, hardware de seguridad, etc.

Políticas de control de acceso

Según la política de control, se puede clasificar los accesos según se basen en la identidad del usuario o se basen en reglas.

a) Control de acceso basado en la identidad

Cabe establecer diferencias entre los accesos individuales y los accesos grupales:

ƒ Accesos individuales: Se fundamentan en una serie de listas para cada recurso, a los cuales pueden acceder los usuarios indicando los derechos que poseen. Así, tendríamos por ejemplo que: Un recurso X puede ser accedido por un usuario A, que tiene derechos de lectura y escritura, y por un usuario B, que tiene solamente derechos de lectura.

ƒ Accesos grupales: Los derechos se brindan a los grupos de usuarios previamente definidos. De esta manera, varios usuarios que puedan tener los mismos derechos frente a un recurso son identificados por un nombre único, facilitando así las tareas de administración y auditoría.

b) Control de acceso basado en reglas

Hay distintos métodos para controlar el acceso a los recursos basado en reglas. Por ejemplo:

ƒ Multinivel: Se definen niveles para los accesos, basándose en parámetros acordados previamente, tales como la fecha de creación, la ubicación física del recurso, etc., generándose a su vez diversos niveles como: restringido, confidencial, secreto, etc.

ƒ Control multiusuario: Se necesita la presencia de ciertos usuarios con derechos previamente determinados para acceder al recurso.

ƒ Basado en el contexto: Se orientan en factores externos como por ejemplo: la hora de acceso, la ubicación del usuario, etc.

Mecanismos de control de acceso

Conocidas las políticas de control de acceso, pasaremos a tratar los mecanismos de control de acceso.

a) Listas de control de acceso

Una lista de control de accesos representa los derechos de los usuarios en una matriz, Este mecanismo es útil para un grupo reducido de usuarios y de recursos, y cuando éstos tienden a ser estables.

b) Etiquetas

Esta técnica se emplea en ambientes con políticas multiniveles. Cada recurso tiene asignada una etiqueta que identifica su clasificación en el sistema. Además, cada usuario recibe una etiqueta, en función de sus privilegios, que se transmitirá junto con la solicitud de acceso. Luego, el recurso comparará las etiquetas y aplicará las políticas de seguridad respectivas.

c) Mecanismos basados en passwords

Mediante un password se autoriza al usuario a acceder al recurso solicitado. Es el método más conocido, pero posee las mismas debilidades que las del servicio de autenticación por passwords.

d) Control de acceso en redes de comunicaciones y control de rutas

En el caso de redes de comunicaciones se deben añadir dos casos importantes:

ƒ Control de acceso a la conexión: Mediante el cual se controla si dos sistemas pueden establecer una comunicación entre ellos.

ƒ Control de acceso de la información a la red: Mediante el cual se establece si un tipo de in formación puede ingresar a un sistema. Por su parte, los mecanismos de control de rutas garantizan que la información viaje sólo por determinadas rutas, redes o subredes, con ciertos atributos de seguridad.

Confidencialidad e integridad

Cada una de las tareas antes mencionadas es distinta, sin embargo, ambas se relacionan y complementan. Se definen de la siguiente manera: La confidencialidad consiste en asegurar que la información no sea revelada a personas no autorizadas. La integridad de la información busca proteger los datos para evitar que sean modificados, alterados o borrados por agentes sin autorización.

En esta sección se tratará acerca de los medios y mecanismos para brindar ambas características.

Confidencialidad

La confidencialidad de la información no sólo implica evitar que se revele el contenido de los mensajes, también significa proteger la información en relación con el tamaño y las variaciones dinámicas de que puede ser objeto: creación, modificación, envío o recepción.

La confidencialidad se puede brindar de dos maneras distintas:

ƒ En el primer caso, se prohíbe al intruso cualquier tipo de acceso a la información. A esto se le denomina control de acceso.

ƒ En el segundo caso, se permite al intruso observar una representación de la información, pero esta representación es tal, que no podrá deducir el contenido. A este método se le denomina encubrimiento de la información.

El método de control de acceso para asegurar la confidencialidad de la información involucra una serie de contramedidas como:

- ✓ ƒ Mecanismos de control de acceso, que filtren las peticiones de cualquier agente que desee acceder a la información.
- ✓ ƒ Control de flujo, que regula el flujo de información de sistemas protegidos a sistemas menos protegidos.
- ✓ ƒ Tecnologías de transmisión con protección de la información, basadas en técnicas de espectro disperso.
- ✓ ƒ Protección contra las emanaciones electromagnéticas de los sistemas.

Mecanismos de Confidencialidad

Son todas aquellas acciones que aseguren la confidencialidad de la información. Entre ellas están:

a) Encriptación

Proporciona medios para convertir un bloque de información en un bloque cifrado y viceversa, mediante el empleo de claves conocidas en los puntos de encriptación y desencriptación.

b) Encubrimiento del tamaño (Data padding)

Con la finalidad de no dar a conocer el tamaño del mensaje se emplean técnicas de encubrimiento, tales como añadir bits a la información antes de su encriptación.

c) Encubrimiento del tráfico (Traffic padding)

Al igual que con los datos, se procura no revelar la cantidad de tráfico generado. Para ello, se suelen aumentar bits a los mensajes que han de transmitirse o se transmiten cadenas adicionales de relleno. Esta técnica se complementa con la encriptación y debe realizarse de forma tal que permita al receptor distinguir la información de los datos de relleno.

Integridad

Los servicios de integridad de la información protegen a ésta contra la modificación, pérdida o substitución, ya sea accidental o intencional. La integridad de la información se puede brindar de dos modos: En el primero, se prohíbe al intruso cualquier oportunidad de modificar la información (control de acceso). En el segundo, se permite al intruso modificar la información, pero se asegura que las modificaciones sean detectadas y corregidas. Este método se denomina detección de corrupción de la información. Las técnicas de control del acceso para asegurar la integridad de la información son similares a las descritas para el caso de confidencialidad. Para la detección de la corrupción de la información hay dos modos de recuperar la información. En el primero, se avisa al receptor que la información fue modificada, para que él tome las medidas pertinentes.

Conceptos de no-repudiación

El servicio de no repudiación ampara al usuario en caso que otro usuario, con el cual estableció una conexión, niegue que ocurrió ésta. Según el escenario de prestación del servicio podemos hablar de:

a) No repudiación del origen

Empleado en caso de desacuerdo sobre si un mensaje determinado fue originado por una de las partes o sobre la fecha en que éste se produjo.

b) No repudiación de la recepción

Empleado en caso de desacuerdo sobre la recepción de un mensaje determinado o la fecha en que ocurrió esa recepción.

Firewalls

Cuando se conecta a Internet una compañía, se crea un punto de acceso de doble sentido dentro de la información confidencial de ésta. Para prevenir el acceso no autorizado desde Internet a los datos de la compañía hay un software especializado llamado Firewall. Esta aplicación opera usualmente sobre un servidor dedicado, que está conectado pero está fuera de la red corporativa. Todos los paquetes que entran a la red a través de firewalls son filtrados o examinados para ver si los usuarios tienen autorización para acceder a ciertos archivos o servicios, o si la información contenida en los mensajes cumple con los criterios empresariales para ser aceptados en la red interna.

Los firewalls proveen una capa de aislamiento entre la red interna y la red externa. Se asume en este escenario que todas las amenazas vienen del mundo exterior. Evidentemente, según las estadísticas esto no siempre es así. Además, las amenazas posteriores pueden ingresar por otro lugar, tal como un acceso de módem vía red telefónica conectada, que no esté controlado o monitorizado. Por otro lado, los firewalls incorrectamente implementados pueden exacerbar la situación creando nuevos –y algunas veces no detectados– agujeros en la seguridad.

Se ha estimado que el 50 % de los crímenes de cómputo son cometidos por los propios empleados de la empresa o ex empleados. Cuando una red se conecta a redes públicas, como Internet, es importante protegerla de los intrusos. La manera más efectiva de proteger los enlaces inseguros es colocar un firewall entre la red local e Internet. Existen diversas tecnologías para implementar un firewall. La principal diferencia entre ellas es la manera cómo analizan la información e implementan las restricciones. Otra dificultad de los firewalls es que no hay normas para su funcionalidad, arquitectura o interoperatibilidad.

Tipos de firewalls

A continuación estudiaremos las siguientes clases de firewalls, su funcionalidad y su arquitectura:

Firewall de filtro de paquetes

Usualmente, esta tecnología se implementa en los routers para filtrar los paquetes cuando pasan entre sus interfaces. Estos routers filtran los paquetes IP basándose en los siguientes criterios:

- ✓ Dirección IP de origen.
- ✓ Dirección IP de destino.
- ✓ Puerto TCP/UDP de origen.
- ✓ Puerto TCP/UDP de destino.

Para bloquear las conexiones desde o hacia un determinado servidor o red, los filtros pueden ser aplicados de varios maneras, incluyendo el bloqueo de conexiones a determinados puertos. Por ejemplo, se puede bloquear todas las conexiones hacia el servidor web, excepto aquellas que utilicen el puerto 80 correspondiente al servicio HTTP. También se puede establecer un filtro para que sólo el tráfico SMTP llegue al servidor de correo. Un filtro es un programa que examina la dirección fuente y la dirección destino de cada paquete que ingrese al servidor de firewalls. Los dispositivos de acceso a la red conocidos como routers también pueden filtrar los paquetes de datos.

Los gateways de filtrado de paquetes pueden implementarse en los routers, es decir que una pieza existente de tecnología puede usarse con los mismos propósitos. Sin embargo, mantener las tablas de filtrado y las reglas de acceso sobre múltiples routers no es fácil y el filtrado de paquetes tiene limitaciones en cuanto a su nivel de seguridad. Los firewalls dedicados, con filtrado de paquetes, son usualmente más fáciles de configurar y requieren menos conocimiento de los protocolos que se vayan a filtrar. Los hackers pueden vencer a los filtros de paquetes con una técnica llamada IP spoofing (engaño de dirección IP). Como los paquetes de filtro orientan sus decisiones de filtrado basándose en direcciones IP de fuente y destino, si un hacker puede hacer que un paquete simule provenir de una dirección IP autorizada o confiable, entonces podría pasar a través del firewall

Gateways de aplicación

Son conocidos también como filtros en el nivel de aplicación, gateways de aplicación o proxies. Estos dispositivos examinan los paquetes en el nivel de aplicación del modelo OSI y van más allá de los filtros de nivel de puerta en su intento de prevenir los accesos no autorizados a los datos corporativos. Mientras los filtros de nivel puerta determinan la legitimidad de las partes que están solicitando la información, los filtros de nivel de aplicación verifican la validez de lo que estas partes solicitan. Los filtros de aplicación examinan toda la solicitud de datos y no sólo las direcciones de fuente y destino. Los archivos asegurados se marcan de tal modo que los filtros de nivel de aplicación impiden que ellos se transfieran a usuarios no autorizados por los filtros de nivel de puerta.

Un firewall basado en esta tecnología sólo permite el paso de los servicios para los cuales exista un proxy, un código escrito especialmente para ejecutar un servicio. Es decir, si un gateway de aplicación sólo contiene proxies para FTP y TELNET, entonces sólo se permitirá el tráfico FTP y TELNET en la red interna y los demás servicios serán bloqueados. Esto brinda mayor seguridad a la red, pero a la vez reduce la escalabilidad y el soporte para nuevas aplicaciones.

Firewall de confianza (trusted gateway)

Se llama gateway de confianza (trusted gateway) a un firewall alternativo que busca liberar toda la confiabilidad sobre el gateway de aplicación para todas las comunicaciones entrantes y salientes. En este caso, se asume que ciertas aplicaciones son confiables y se les permite rodear (bypass) al gateway de aplicación totalmente y establecer las conexiones directamente, en vez de que éstas se ejecuten a través del proxy. Así, los usuarios externos pueden acceder a los servidores de información y servidores WWW sin colgarse a las aplicaciones proxy del gateway.

Los proxies también pueden proveer o negar conexiones basadas en direccionalidad. A los usuarios puede permitírseles cargar archivos, mas no descargarlos. Algunos gateway de nivel de aplicación pueden encriptar las comunicaciones sobre esas conexiones establecidas. El nivel de dificultad atribuido a configurar un gateway de nivel de aplicación versus un filtro basado en router es discutible. Los gateways basados en router requieren conocer de cerca el comportamiento de los protocolos, mientras que los gateway de nivel de aplicación tratan con los protocolos de nivel más alto, es decir de capa de aplicación. Los proxies introducen una mayor latencia comprados con los filtros de nivel puerta. La debilidad clave de un gateway de nivel de aplicación es que no detecta código malicioso indebido, como un programa de caballo de Troya o un macro virus.

Autenticación biométrica

Si la seguridad ofrecida por la autenticación de Token es insuficiente, existe la autenticación biométrica, basada en huellas digitales, impresiones de la palma de la mano, patrones de la retina, reconocimiento de voz u otras características físicas. Los password y las tarjetas inteligentes pueden ser robados, más no las huellas digitales ni los patrones de la retina. Todos los dispositivos de autenticación biométrica exigen que todos los usuarios válidos se registren primero guardando copias de sus huellas digitales, voz o patrones de su retina en una base de datos de

validación. Ésta brinda al dispositivo biométrico la referencia cada vez que el usuario intenta un acceso al sistema.

Los dispositivos de autenticación biométrica no están perfeccionados aún ni hechos a prueba de tontos. Todos estos dispositivos deben calibrarse para tener la adecuada sensibilidad. Si el algoritmo de comparación del dispositivo biométrico está programado muy sensiblemente, entonces ocurrirán falsos rechazos de usuarios válidos debido a ligeras variaciones detectadas entre la característica de referencia biométrica y la muestra actual. Si el dispositivo no está suficientemente calibrado en su sensibilidad, entonces se producirán aceptaciones falsas y se permitirá el ingreso de impostores, debido a que las comparaciones no estaban lo suficientemente detalladas.