Indice

Contenido Pagina

Introducción 4

Condiciones Generales 5

Protocolos de Red 6

Puertos de Protocolos 15

Encriptación de Datos 17

Firma Digital 18

Bases de Datos 20

Cookies 26

Ataque y Defensa 30

Conclusión 32

Bibliografía 33

Introducción

Cuando entra en Internet, está entrando en una gran sociedad en línea. Y, como en toda sociedad humana, no todo es agradable. En el mundo en línea existen amenazas a la seguridad, igual que en el resto del mundo. Si aprende a protegerse (a proteger su equipo y sus datos), se asegurará que el tiempo que pase en línea será productivo y divertido.

Condiciones iniciales

Dentro de la seguridad se deben considerar algunos mecanismos en los distintos aspectos de esta área como:

Seguridad Física.

Para considerar la seguridad física se pueden implementar diversos mecanismos tales como:

A nivel preventivo

- Acceso controlado al equipo en base a diversas políticas tales como

- Uso del equipo por personal autorizado (regla)
- Solo podrá tener acceso al equipo aquel personal que cuente con conocimientos mínimos sobre computación (política)

- El personal que carezca de todo conocimiento podrá solicitar la ayuda del centro de información o de los analistas de sistemas para hacer uso del equipo del sistema
- Introducción de clave personal del usuario mediante la portación de una tarjeta con sus datos personales e historial la cual se aloja en una base de datos de todo el personal el cual da seña de su estado y condición dentro de la empresa. Esto con el objetivo de saber el uso exacto de cada equipo y por parte de cada usuario.

- Respaldo continuo de la información al poder contar con mas de un servidor de base de datos lo cual asegure la integridad total de la información.

- Ubicación de las instalaciones que cumplan con normas internacionales de calidad (ISO 9000)

- Control de alarma la cual notifique en todo momento sobre la integridad física del sistema

A nivel correctivo

- El aseguramiento del equipo en alguna agencia de seguros para que en caso de posible siniestro no exista una perdida total por parte de los elementos físicos que controlan y dan soporte al sistema.

Seguridad Lógica

La seguridad lógica al referirse a controles lógicos dentro del software se implementa mediante la construcción de contraseñas en diversos niveles de los sistemas donde permita solo el acceso en base a niveles de seguridad de usuarios con permiso, en base al sistema operativo que use como plataforma el sistema a implantarse puedo considerar además a nivel código, algoritmos que generen claves para poder encriptar los archivos de contraseñas dentro del sistema lo cual me permita mayor seguridad en un entorno de red. Generar un módulo del sistema para la emisión de reportes para el administrador del sistema en donde se muestre tablas de uso del sistema así como los usuarios y los niveles de acceso por parte de los tales para poder determinar el uso y acceso al sistema.

También es necesario contar con el diseño de módulos que ejecuten un Control de alarma la cual notifique en todo momento sobre la integridad de la información del sistema

Protocolos de Red

TCP/IP

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, en lugar de ser uno de los estándares definidos por la ISO, IICC, etc...

Esta arquitectura se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU.), y con la expansión de la INTERNET se ha convertido en una de las arquitecturas de redes más difundida.

Antes de continuar, pasemos a ver la relación de esta arquitectura con respecto al modelo de referencia OSI (Open Systems Interconnection) de la ISO. Así como el modelo de referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por 4 niveles:

- **Nivel de subred** [enlace y físico]
- **Nivel de interred** [Red, IP]
- **Protocolo proveedor de servicio** [Transporte, TCP o UDP]
- **Nivel de aplicación**.

El protocolo Internet (*Internet Protocol − IP*)

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más específica como datagrama Internet o datagrama IP

Las características de este protocolo son:

- No orientado a Conexión
- Transmisión en unidades denominadas **datagramas**.
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

La entrega del datagrama en IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensamblar los fragmentos del mensaje. Por otra parte, el IP no contiene suma de

verificación para el contenido de datos del datagrama, solamente para la información del encabezado.

Las aplicaciones

Hay una serie de protocolos implementados dentro de TCP/IP:

- Protocolo sencillo de transferencia de correo (SMTP) :Es un protocolo de servicio de correo electrónico, listas de correo, etc...y su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante TCP/IP.
- Protocolo de transferencia de ficheros (FTP) : Permite el envío y recepción de ficheros de cualquier tipo de o hacia un usuario. Cuando se desea el envío, se realiza una conexión TCP con el receptor y se le pasa información sobre el tipo y acciones sobre el fichero así como los accesos y usuarios que pueden acceder a él. Una vez realizado esto, se envía el fichero. Finalizado esto, se puede cortar la conexión.
- TELNET : es un protocolo para que dos computadores lejanos se puedan conectar y trabajar uno en el otro como si estuviera conectado directamente. Uno de ellos es el usuario y el otro el servidor. TCP se encarga del intercambio de información.

Un datagrama IP consta de una cabecera y un campo de datos. los campos con que cuenta son los siguientes:

Versión : este campo codifica la versión del protocolo IP. De esta forma se pueden hacer convivir en la red paquetes de datos de diferentes versiones de protocolos. el receptor analizando este campo sabrá como interpretar el resto de la cabecera

IHL : Internet header length (longitud de cabecera Internet) como la cabecera de un datagrama IP no es constante es necesario codificar la longitud de la cabecera en este campo.

Tipo de servicio: este campo define el tipo de servicio que se requiere para la transmisión de ese paquete, por ejemplo si se concede mas importancia a la correccion de errores o a la velocidad de entrega.

Longitud total: este campo contiene la longitud total del datagrama, que tiene un máximo de 64 bytes.

Identificación : cuando un datagrama se divide es necesario que todos los fragmentos lleven la misma identificación. para que el destinatario sepa a que datagrama corresponde cada parte

Bit DF: dont fragment (bit de no fragmentación)cuando este bit esta en uno se le indica a la red que este bit no puede ser fragmentado.

Bit MF: more fragments (bit de mas fragmentos) este bit estará siempre en uno, es por tanto el indicador del ultimo fragmento

Desplazamiento de fragmento: este campo indica en que lugar debe ser insertado el fragmento del datagrama para su ensamblaje correcto

Tiempo de vida: este campo actúa como contador que determina la vida que le queda a cada paquete en la red, cuando el contador se hace cero el encaminador drena el paquete en la red.

Protocolo : indica el protocolo de transporte que ha generado el datagrama (TCP)

Código de redundancia: este campo lleva el control de cabecera del paquete IP

Dirección fuente: codifica la dirección de donde se produce el paquete

Dirección destino: codifica la dirección del destinatario

Opciones : este campo se utiliza se utiliza para futuras versiones del IP

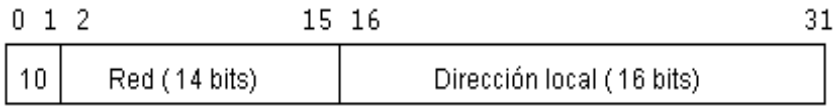
Direccionamiento IP

El TCP/IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada. Únicamente el NIC (Centro de Información de Red) asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, dicha red puede determinar su propio sistema de numeración. Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red.

Las direcciones de Clase A corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.1.0.0 hasta la 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

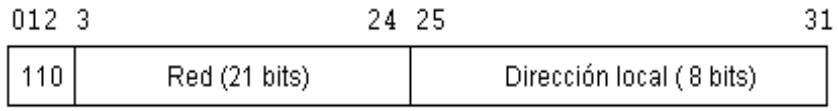
Clase A

Las direcciones de Clase B sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0. Esto permite tener 16320 redes con 65024 host en cada una.



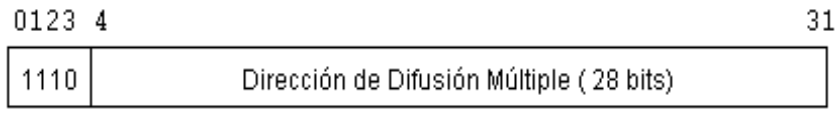
Clase B

Las direcciones de Clase C tienen sólo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, lo que permite cerca de 2 millones de redes con 254 hosts cada una.



Clase C

Por último, las direcciones de Clase D se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.



Clase D

IPv6

Es la nueva versión del protocolo IP, utiliza campos de dirección de 128 bits extendiendo la cantidad de direcciones IP disponibles para satisfacer la gran cantidad de dispositivos de Internet en el futuro. IPv6 implementa junto con el protocolo IPv4 que aumenta la funcionalidad y compatibilidad del Sistema Operativo.

Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, con un total de 32 bits.

Por comodidad estos bits se representan como si estuviesen separados por un punto, por lo que el formato de dirección IP puede ser red.local.local.local para Clase A hasta red.red.red.local para clase C.

Mensajes de error y control en IP (ICMP)

El Protocolo Internet (IP) proporciona un servicio de entrega de datagramas, no confiable y sin conexión, al hacer que cada router direccione datagramas. Si un router no puede, por ejemplo, rutear o entregar un datagrama, o si el router detecta una condición anormal que afecta su capacidad para direccionarlo (v.q., congestionamiento de la red), necesita informar a la fuente original para que evite o corrija el problema.

Para permitir que los routers de una red reporten los errores o proporcionen información sobre circunstancias inesperadas, se agregó a la familia TCP/IP un mecanismo de mensajes de propósito especial, el *Protocolo de Mensajes de Control Internet* (**ICMP**). El ICMP permite que los routers envíen mensajes de error o de control hacia otros routers o anfitriones, proporcionando una comunicación entre el software de IP en una máquina y el mismo software en otra.

Cuando un datagrama causa un error, el ICMP sólo puede reportar la condición del error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

Formato de los mensajes ICMP:

Aunque cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo TYPE (TIPO) de mensaje, de 8 bits y números enteros, que identifica el mensaje; un campo CODE (CODIGO), de 8 bits, que proporciona más información sobre el tipo de mensaje, y una campo CHECKSUM (SUMA DE VERIFICACIÓN), de 16 bits. Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema.

La razón de regresar más que el encabezado del datagrama únicamente es para permitir que el receptor determine de manera más precisa qué protocolo(s) y qué programa de aplicación son responsables del datagrama.

El campo TYPE de ICMP define el significado del mensaje así como su formato. Los tipos incluyen:

CAMPO TYPE Tipo de Mensaje ICMP

0 Respuesta de ECO

3 Destino inaccesible

4 Disminución de origen (source quench−datagrama eliminado por congestión)

5 Redireccionar (cambiar una ruta)

8 Solicitud de ECO

11 Tiempo excedido para un datagrama

12 Problema de parámetros de un datagrama

13 Solicitud de TIMESTAMP

14 Respuesta de TIMESTAMP

15 Solicitud de Información (obsoleto)

16 Respuesta de Información (obsoleto)

17 Solicitud de Máscara de dirección

18 Respuesta de máscara de dirección

Protocolo de Datagrama de Usuario (UDP).

El UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. Esto es, además de los datos, cada mensaje UDP contiene tanto en número de puerto de destino como el número de puerto origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe una respuesta.

El UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. En resumen:

El UDP proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para transportar mensajes entre máquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de la computadora anfitrión.

Formato de los mensajes UDP:

Cada mensaje UDP se conoce como *datagrama de usuario.* Conceptualmente, un datagrama de usuario consiste en dos partes: un encabezado UDP y un área de datos UDP. El encabezado se divide en cuatro campos de 16 bits, que especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP.

Protocolo de Control de Transmisión (TCP)

Servicio de Transporte de Flujo Confiable

Hemos visto el servicio de entrega de paquetes sin conexión y no confiable, que forma la base para toda comunicación en Internet, así como el protocolo IP que lo defina.

Ahora veremos el segundo servicio más importante y mejor conocido a nivel de red, la entrega de flujo confiable (Reliable Stream Transport), así como el Protocolo de Control de Transmisión (TCP) que lo define.

En el nivel más bajo, las redes de comunicación proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir debido a errores (falla el hardware, sobrecarga de la red,...). Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega de conexión y no confiable para transferencias de grandes volúmenes de información resulta ser la peor opción. Debido a esto, el TCP se ha vuelto un protocolo de

propósito general para estos casos.

AppleTalk

AppleTalk es el nombre de la red entre iguales, diseñada por Apple Computer Corporation, para su utilización en computadores Macintosh y, más recientemente, en Power Mac. El diseño original se pensó para permitir que se compartan ficheros e impresoras entre los usuarios de la red, de modo que su configuración fuera muy sencilla, lo que permitiría beneficiarse cualquier usuario no experto de los servicios de la red.

El primer diseño de Apple Talk fue una sencilla red que resolvía la conexión de un Macintosh a una impresora, sin embargo, con Apple Talk se pueden confeccionar redes muy amplias y complejas.

A continuación veremos esquematizado la arquitectura de protocolos que son utilizados por Apple Talk y su relación con las capas del modelo OSI.

A continuación describiremos brevemente algunos de estos protocolos ya mencionados en el esquema:

- **ALAP** (AppleTalk Link Access Protocol)
- **ELAP** (Ethernet Link Access Protocol)
- **TLAP** (Token Link Access Protocol) son los protocolos de nivel de enlace utilizados por AppleTalk, quien utilizara uno u otro dependiendo de la capa física.
- **DDP** (Datagram Delivery Protocol) es el protocolo de AppleTalk en el nivel de Red que se encarga de encaminar los data gramas de modo semejante al protocol IP de las redes UNIX. Las tablas de encaminamiento entre los diferentes encaminadores o routers se mantienen a través de un protocolo denominado RTMP (Routing Table Maintenance Protocol).
- **NBP** (Name Binding Protocol) es protocolo situado en la capa de transporte que se encarga de asociar nombres de servicios con direcciones, de modo que los usuarios puedan utilizar nombres nemotécnicos para solicitar los servicios de la red.
- **ATP** (AppleTalk Translation Protocol) es el protocolo de transporte encargado de realizar conexiones seguras en AppleTalk. Equivalente al TCP de la red UNIX.
- **ZIP** (Zone Information Protocol) es un protocolo asociado a la capa de sesión que se encarga del gobierno de las zonas AppleTalk
- **ASP** (AppleTalk Session Protocol) es el protocolo de sesión encargado del gobierno de las sesiones, que elimina paquetes duplicados y los ordena según su numero de secuencia.
- **PAP** (Printer Access Protocol) proporciona en el nivel de sesión los servicios de impresora para toda la red.

En las capas superiores aparecen protocolos como **AFP** para el intercambio de ficheros, y, **PostScript** como lenguaje descriptor de documentos con que alimentar las impresoras. **AppleShare** y **LaserShare** se encargan de hacer de modo transparente al usuario (Nivel de Aplicación) del servicio de ficheros y de dispositivos de impresión, de modo que al usuario le parecen locales los discos, carpetas o impresoras que, en realidad, son remotos.

Puertos de Protocolo

TCP/IP bajo UDP

La mayoría de los Sistemas Operativos actuales soportan multiprogramación. Puede parecer natural decir que un proceso es el destino final de un mensaje. Sin embargo, especificar que un proceso en particular en una máquina en particular es el destino final para un datagrama es un poco confuso.

En vez de pensar en un proceso como destino final, imaginaremos que cada máquina contiene un grupo de puntos abstractos de destino, llamados ***puertos de protocolo***. Cada puerto de protocolo se identifica por medio de un número entero positivo.

Para comunicarse con un puerto externo, un transmisor necesita saber tanto la dirección IP de la máquina de destino como el número de puerto de protocolo del destino dentro de la máquina.

El UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. Esto es, además de los datos, cada mensaje UDP contiene tanto en número de puerto de destino como el número de puerto origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe una respuesta.

El UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. En resumen:

El UDP proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para transportar mensajes entre máquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de la computadora anfitrión.

Puertos, conexiones y puntos extremos

Al igual que el UDP, el TCP reside sobre el IP en el esquema de estratificación por capas de protocolos. El TCP permite que varios programas de aplicación en una máquina se comuniquen de manera concurrente y realiza el demultiplexado del tráfico TCP entrante entre los programas de aplicación. Así mismo, al igual que el UDP, el TCP utiliza números de ***puerto de protocolo*** para identificar el destino final dentro de una máquina. Cada puerto tiene asignado un número entero pequeño utilizado para identificarlo.

Para comprender el significado de un puerto hay que pensar de cada puerto como en una cola de salida en la que el software de protocolo coloca los datagramas entrantes, aunque en realidad los puertos TCP son más complejos, ya que un número de puerto no corresponde a un sólo objeto. El TCP utiliza la conexión, no el puerto de protocolo, como su abstracción fundamental; las conexiones se identifican por medio de un par de puntos extremos.

¿Qué es exactamente un punto extremo en TCP?

Un punto extremo es un par de números enteros **(host, puerto)**, en donde *host* es la dirección IP de un anfitrión y *puerto* es el un puerto TCP en dicho anfitrión.

Las conexiones vienen definidas por dos puntos extremos, y es más: la abstracción de la conexión para TCP permite que varias conexiones compartan un punto extremo (por ejemplo, varias conexiones en los mismos puertos). Esto es posible a que el TCP identifica una conexión por medio de un par de puntos extremos, y por

eso varias conexiones en la misma máquina pueden compartir un número de puerto TCP.

El TCP combina la asignación dinámica y estática de puertos mediante un conjunto de *asignación de puertos bien conocidos* para programas llamados con frecuencia, pero la salida de la mayor parte de los números disponibles para el sistema se asigna conforme los programas lo necesitan.

La siguiente tabla muestra un ejemplo de números de puerto TCP asignados actualmente.

DECIMAL	CLAVE	CLAVE UNIX	DESCRIPCIÓN
0			Reservado
1	TCPMUX		Multiplexor TCP
5	RJE		Introducción de función remota
7	ECHO	echo	Eco
9	DISCARD	discard	Abandonar
11	USERS	systat	Usuarios activos
13	DAYTIME	daytime	Fecha, hora
15		netstat	Estado de red
17	QUOTE	qotd	Cita del día
19	CHARGEN	chargen	Generador de caracteres
20	FTP−DATA	ftp−data	Datos para FTP
21	FTP	ftp	File Transfer Protocol
23	TELNET	telnet	Conexión por terminal
25	SMTP	smtp	Protocolo de Transporte de Correo Sencillo
42	NAMESERVER	name	Nombre del host servidor
43	NICNAME	whois	Comando whois
53	DOMAIN	nameserver	Servidor de nombre de dominio (DNS)
79	FINGER	finger	Comando finger
93	DCP		Protocolo de Control de Dispositivo
101	HOSTNAME	hostnames	Servidor de Nombre de Anfitrión NIC
103	X400	x400	Servicio de correo X400
104	X400−SND	x400−snd	Envío de coreo X400

Encriptación de Datos

Como sabemos, en un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos.

Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encriptación de Datos.

Métodos de encriptación:

Para poder Encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes:

Los algoritmos HASH, los simétricos y los asimétricos.

- **Algoritmo HASH:**

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

- **Algoritmos Simétricos:**

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactuan varios interlocutores.

- **Algoritmos Asimétricos (RSA):**

Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir. El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro.

El usuario, ingresando su PIN genera la clave Publica y Privada necesarias. La clave Publica podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada.

Cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la Clave Publica porque el utilizó su Clave Privada.

Firma Digital

Descripción

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Es la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmen6te por intermedio de redes de computadoras le dio lugar al concepto. Pero sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas (jurídicas o reales).

Se intenta hacer coincidir el modelo de firma digital con los requerimientos y virtudes que debe tener una firma y así darle validez a esta mecánica. El fin es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado.

El papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.). Esta cualidad física le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará señales identificables.

Pero estas mismas cualidades traen aparejados inconvenientes que el uso de sistemas de computación podría evitar. Ciertamente los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/o al rescatarlos), y el compartir los documentos también resulta inconveniente.

Ventajas Ofrecidas por la Firma Digital

El uso de la firma digital satisface los siguientes aspectos de seguridad:

- Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

- Autenticidad del origen del mensaje*:* este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

- No repudio del origen*:* el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Aspectos técnicos

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original más la firma digital se lo denominará mensaje.

Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original.

En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública−privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido.

A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional:

- Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad).

- Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad).

- El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante

la evidencia de la firma (no repudio).

Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.

Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, solo puede ser desencriptado por la clave pública.

Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma.

Si bien no se trata de un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye.

Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad y no repudio del origen), pero no se satisface el concepto de confidencialidad de la información (secreto)

Bases de Datos para Web

Una Base de Datos es, esencialmente, un conjunto de datos ordenados en filas y columnas que se cargan y se ven en un programa de Planilla de Cálculos. Cada dato esta compuesto por un grupo de informaciones llamadas campos; entonces podemos decir que una base de datos es un banco de informaciones ordenadas en filas y columnas. Los campos varían de acuerdo al rubro y el universo seleccionados.

Base de datos distribuida

Una Base de Datos Distribuida es, una base de datos construida sobre una red computacional y no por el contrario en una máquina aislada. La información que constituye la base de datos esta almacenada en diferentes sitios en la red, y las aplicaciones que se ejecutan accesan datos en distintos sitios.

Una Base de Datos Distribuida entonces es una colección de datos que pertenecen lógicamente a un sólo sistema, pero se encuentra físicamente esparcido en varios "sitios" de la red. Un sistema de base de datos distribuidas se compone de un conjunto de sitios, conectados entre sí mediante algún tipo de red de comunicaciones, en el cual:

- Cada sitio es un sistema de base de datos en sí mismo, pero,
- Los sitios han convenido en trabajar juntos (si es necesario) con el fin de que un usuario de cualquier sitio pueda obtener acceso a los datos de cualquier punto de la red tal como si todos los datos estuvieran almacenados en el sitio propio del usuario.

En consecuencia, la llamada "*base de datos distribuida*" es en realidad una especie de objeto virtual, cuyas partes componentes se almacenan físicamente en varias bases de datos "reales" distintas ubicadas en diferentes sitios. De hecho, es la unión lógica de esas bases de datos. En otras palabras, cada sitio tiene sus propias bases de datos "reales" locales, sus propios usuarios locales, sus propios DBMS y programas para la administración de transacciones (incluyendo programas de bloqueo, bitácoras, recuperación, etc), y su propio

administrador local de comunicación de datos (administrador DC). En particular un usuario dado puede realizar operaciones sobre los datos en su propio sitio local exactamente como si ese sitio no participara en absoluto en el sistema distribuido (al menos, ése es uno de los objetivos). Así pues, el sistema de bases de datos distribuidas puede considerarse como una especie de sociedad entre los DBMS individuales locales de todos los sitios. Un nuevo componente de software en cada sitio (en el aspecto lógico, una extensión del DBMS local) realiza las funciones de sociedad necesarias; y es la combinación de este nuevo componente y el DBMS ya existente lo que constituye el llamado "sistema de administración de bases de datos distribuidas" (DDBMS, distributed database management system).

[Base de Datos Distribuidas]

Conceptos básicos.

El sistema de administración de Base de Datos Distribuida (DDBMS), esta formado por las transacciones y los administradores de base de datos distribuidos de todas las computadoras. Tal DDBMS en un esquema genérico implica un conjunto de programas que operan en diversas computadoras. Estos programas pueden ser subsistemas de un producto único DDBMS, concesionado por un sólo fabricante, o también pudiera resultar de una colección de programas de fuentes dispares: algunos considerados por fabricantes y algunos otros escritos en casa.

Un administrador de base de datos (DTM) es un programa que recibe solicitudes de procesamiento de los programas de consulta o de transacciones y a su vez las traduce en acciones para los administradores de la base de datos. Una función importante del DTM es coordinar y controlar dichas acciones. · Cada sitio tiene sus propias bases de datos "reales" locales, sus propios usuarios locales, sus propios DBMS y programas para administración de transacciones y su propio administrador local de comunicación de datos. La diferencia principal entre los sistemas de bases de datos centralizados y los distribuidos es que en los primeros, los datos residen en una sola localidad, mientras que, en lo últimos, se encuentran en varias localidades. Cada localidad puede procesar transacciones locales, es decir, aquellas que sólo acceden a datos que residen en esa localidad. Además, una localidad puede participar en la ejecución de transacciones globales, es decir, aquellas que acceden a datos de varias localidades, ésta requiere comunicación entre las localidades. · Una transacción local es la que accede a cuentas en la localidad individual donde se inicio. En cambio, una transacción global accede a cuentas de una localidad distinta a la localidad donde se inicio o a cuentas de varias localidades diferentes.

¿Por qué son deseables las bases de datos distribuidas?

La respuesta básica a esta pregunta es que por lo regular las empresas ya están distribuidas, por lo menos desde el punto de vista lógico (en divisiones, departamentos, proyectos, etc.) y muy probablemente en el sentido físico también (en plantas, talleres, laboratorios, y demás), de lo cual se desprende que en general la información ya está también distribuida, porque cada unidad de organización dentro de la empresa mantendrá por fuerza los datos pertinentes a su propio funcionamiento. Así pues, un sistema distribuido permite que la

estructura de la base de datos refleje la estructura de la empresa: los datos locales se pueden mantener en forma local, donde por lógica deben estar, pero al mismo tiempo es posible obtener acceso a datos remotos en caso necesario.

Un Panorama de las Bases de Datos Orientadas a Objetos

Como cualquier base de datos programable, una base de datos orientada a objetos (BDOO) da un ambiente para el desarrollo de aplicaciones con un depósito persistente listo para su explotación. Una BDOO almacena y manipula información que puede ser digitalizada (representada) como objetos, proporciona una estructura flexible con acceso ágil, rápido, con gran capacidad de modificación. Además combina las mejores cualidades de los archivos planos, las bases jerárquicas y relaciónales.

Actualmente, el creciente uso de las metodologías de programación orientadas a objetos está promoviendo la aparición de manejadores de BDOO en el mercado. Esto tiene sentido, puesto que la tecnología de objetos proviene del desarrollo de metodologías avanzadas de programación. Más aún, la comunidad internacional está convencida de que los manejadores de BDOO tienen la flexibilidad tanto en la definición del modelo de datos como en el desempeño tan anhelado por muchos desarrolladores de aplicaciones, lo que es imposible encontrar en los modelos jerárquicos de red o relaciónales.

Aspectos de Tecnología

Los objetos pueden estar compuestos por cualquier tipo de información que, eventual mente, puede almacenarse en forma digital; por ejemplo, imágenes barridas, voz, sonido, dibujos, planos arquitectónicos complejos, esquemas electrónicos y diagramas desarrollados por ingenieros, así como los tradicionales tipos de datos alfanuméricos. Comúnmente, las aplicaciones que producen este tipo de objetos complejos, al terminar, los guardan en archivos de datos en distintos formatos. Cuando el programa es reactivado, los objetos, se cargan nuevamente. En estos ambientes, los objetos son accesibles sólo a un usuario en cada momento, no existen mecanismos de seguridad, no hay manera de protegerse ante la eliminación accidental de un objeto complejo. Las BDOO superan todas estas dificultades porque permiten que múltiples usuarios compartan objetos complejos para manipularlos en ambiente seguro y estructurado.

Las bases de datos convencionales fueron diseñadas para manejar tipos de datos alfanuméricos, por ello, difícilmente pueden usar objetos y métodos. Algunos proveedores de bases de datos relacionales han respondido a las tendencias de la tecnología facilitando "front−ends" orientados a objetos, una capa filtrante que traduce entre objetos y la base de datos interna. Sin embargo, este enfoque es limitado porque los objetos deben ser interceptados, desmenuzados en una forma que se almacene en la base de datos relacional, lo que resulta en un proceso difícil. Los objetos deben ser repetidamente ensamblados (para trabajar con ellos) y desarticulados (para guardarlos).

Una base de datos de red o jerárquica puede almacenar objetos complejos, pero esta arquitectura no es flexible, lo cual motiva, el uso del modelo relacional. El problema principal con los modelos en red o jerárquicos es que la estructura es definida rígidamente, cuando la base de datos se crea. Estos sistemas casi no permiten flexibilidad para modificaciones, el sistema debe desactivarse cuando se requiere modificar estructuras de objetos o métodos.

Una base de datos relacional tiene una estructura más flexible, pero no puede manejar tipos de datos complejos. Para sobreponerse a estas limitaciones, algunos proveedores han desarrollado las bases de datos orientadas a objetos, las cuales son diseñadas para manipular los objetos con los conceptos de la programación orientada a objetos, proporcionando un concepto persistente en un ambiente multiusuario seguro.

Existen niveles en los cuales las bases de datos incorporan los conceptos alrededor de la metodología de objetos. La primera clase, puede denominarse BDOO pasivas o "estructuralmente orientadas a objetos", que

permiten manejar objetos compuestos. Una base de datos pasiva puede almacenar objetos complejos pero no puede definir comportamientos. Este tipo de bases de datos se utiliza para almacenar objetos de otras aplicaciones. Una BDOO pasiva incluye conceptos como "jerarquía parte de", pero no incluye mecanismos para tipos definidos por el usuario o aspectos que definen comportamientos. Una BDOO es activa u "orientada a objetos por comportamiento" si permite definir y ejecutar comportamiento de los objetos dentro de la base de datos, incorpora conceptos como la "herencia" y permite el manejo de tipos definidos por el usuario. Si se incorporan todos los aspectos se denomina "plenamente orientada a objetos". En bases de datos activas, es sencillo programar una señal de alerta en un objeto inventario cuando se llega a un nivel mínimo.

Ventajas en BDOOs

Entre las ventajas más ilustrativas de las BDOOs está su flexibilidad, soporte para el manejo de tipos de datos complejos. Por ejemplo, en una base de datos convencional, si una empresa adquiere varios clientes por referencia de clientes servicio, pero la base de datos existente, que mantiene la información de clientes y sus compras, no tiene un campo para registrar quién proporcionó la referencia, de qué manera fue dicho contacto, o si debe compensarse con una comisión, sería necesario reestructurar la base de datos para añadir este tipo de modificaciones. Por el contrario, en una BDOO, el usuario puede añadir una "subclase" de la clase de clientes para manejar las modificaciones que representan los clientes por referencia.

La subclase heredará todos los atributos, características de la definición original, además se especializará en especificar los nuevos campos que se requieren así como los métodos para manipular solamente estos campos. Naturalmente se generan los espacios para almacenar la información adicional de los nuevos campos. Esto presenta la ventaja adicional que una BDOO puede ajustarse a usar siempre el espacio de los campos que son necesarios, eliminando espacio desperdiciado en registros con campos que nunca usan.

La segunda ventaja de una BDOO, es que manipula datos complejos en forma rápida y ágilmente. La estructura de la base de datos está dada por referencias (o apuntadores lógicos) entre objetos. No se requieren búsquedas en tablas o uniones para crear relaciones. Esta capacidad resulta atractiva en aplicaciones de la ingeniería, donde las relaciones entre componentes dependen de factores diversos.

Posibles Problemas

Al considerar la adopción de la tecnología orientada a objetos, la inmadurez del mercado de BDOO constituye una posible fuente de problemas por lo que debe analizarse con detalle la presencia en el mercado del proveedor para adoptar su producto en una línea de producción sustantiva. Por eso, en este artículo proponemos que se explore esta tecnología en un proyecto piloto.

El segundo problema es la falta de estándares en la industria orientada a objetos. Sin embargo, el "Object Managenent Group" (OMG), es una organización Internacional de proveedores de sistemas de información y usuarios dedicada a promover estándares para el desarrollo de aplicaciones y sistemas orientados a objetos en ambientes de cómputo en red.

Bases de Datos Relacionales

Las bases de datos relacionales surgen a partir de un artículo de Codd en 1970. Desde entonces es posible encontrarlas en todo centro de cómputo. Muchas aplicaciones y usuarios de bases de datos tienen a su alcance software para el manejo de bases de datos relacionales de muchas marcas comerciales. Los hay para computadoras personales, medianas y grandes.

Pocas veces se reflexiona en cual es el motivo de su éxito y por qué se ha popularizado tanto. Una de las causas principales es el modelo de datos matemático que lo respalda.

Al utilizar una base de datos se está tratando de modelar los datos y sus conexiones en un problema del mundo real. Para definir el modelo relacional se inicia con una definición de lo que es un modelo de datos en general.

Un modelo de datos es un sistema formal y abstracto que permite describir los datos de acuerdo con reglas y convenios predefinidos. Es formal pues los objetos del sistema se manipulan siguiendo reglas perfectamente definidas y utilizando exclusivamente los operadores definidos en el sistema, independientemente de lo que estos objetos y operadores puedan significar [Rivero].

Según el mismo autor, un modelo de datos tiene tres componentes que son:

Componentes:

- Estructuras de datos: es la colección de objetos abstractos formados por los datos.
- Operadores entre las estructuras: el conjunto de operadores con reglas bien definidas que permiten manipular a dichas estructuras.
- Definiciones de integridad: es una colección de conceptos y reglas.
- Que permite expresar que valores de datos pueden aparecer válidamente en el modelo.

Bases de datos orientadas a Internet

Las bases de datos orientadas a Internet tienen como misión el desarrollo del e−commerce, es decir, presentan una insfraestructura completa para el diseño de aplicaciones que toman ventaja de una cantidad creciente de oportunidades que afloran en la comunidad Internet. En general, estas bases de datos cumplen con los estándares de Java (lenguajes de programación orientados a Internet), Corba (aplicaciones distribuidas que utilizan Java para su desarrollo) y HTML (lenguaje de marcas para diseño de páginas web). También estas bases de datos tienen completa funcionalidad con el server Web. Además ofrecen características que no poseen sus pares descritos como interfaces SQL y pre−compiladores pro *C que permiten combinar a los desarrolladores combinar la lógica de procedimientos con SQL para construir aplicaciones complejas para la empresa.

Otra de las características que resaltan la excelencia de las bases de datos es que proveen mecanismos de encriptación dentro de la bases de datos para asegurara la integridad y seguridad de los datos e impedir la fuga de los mismos

Desventajas de las bases de Datos Orientadas Internet

La principal desventaja es que estas bases de datos proporcionan características que son bastantes complejas. Además, muchas de ellas han incorporado tecnología que aun no se encuentra normalizada concretamente como es el caso XML por lo que el desarrollo de muchas de estas aplicaciones pasa a ser una verdadera osadía sin contar con el hecho de que realmente funcionen para todas las plataformas que lo requieran.

Cookies

En los últimos meses las cookies han atraído un interés considerable en publicaciones sobre temas relacionados con los ordenadores, la Internet y la seguridad.

A pesar de que los grupos de anunciantes mantienen una guerra particular con ciertas organizaciones que promueven la intimidad en la Red, lo cierto es que las cookies continúan usándose extensivamente.

La mayoría de los usuarios ya pueden rechazar a voluntad las cookies desde sus navegadores o bien desde un número cada vez mayor de programas y extensiones al navegador que las bloquean. De esta manera son libres de elegir si prefieren la navegación con cookies o sin ellas, de decidir si desean arriesgar su intimidad a

cambio de ciertas comodidades y de una navegación más individualizada.

Con el tiempo se verá cuál es el destino de las cookies, si caerán en el olvido o se convertirán en estándar aceptado para extender las posibilidades del protocolo HTTP.

Lo más importante es que entre tanto los usuarios de Internet sean informados acerca de la naturaleza real de las cookies, quiénes las usan y para qué, y qué riesgo real suponen para su intimidad. Mientras no surjan estándares al respecto, nada como la información para combatir los miedos irracionales.

Descripción

Las cookies constituyen una potente herramienta empleada por los servidores Web para almacenar y recuperar información acerca de sus visitantes. Dado que el protocolo de transferencia de Hipertexto (HTTP) es un protocolo sin estados (no almacena el estado de la sesión entre peticiones sucesivas), las cookies proporcionan una manera de conservar información entre peticiones del cliente, extendiendo significativamente las capacidades de las aplicaciones cliente/servidor basadas en la Web. Mediante el uso de cookies se permite al servidor Web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese servidor, nombre y contraseña, productos que más le interesan, etc.

Una cookie no es más que un fichero de texto que algunos servidores piden a nuestro navegador que escriba en nuestro disco duro, con información acerca de lo que hemos estado haciendo por sus páginas.

Entre las mayores ventajas de las cookies se cuenta el hecho de ser almacenadas en el disco duro del usuario, liberando así al servidor de una importante sobrecarga. Es el propio cliente el que almacena la información y quien se la devolverá posteriormente al servidor cuando éste la solicite. Además, las cookies poseen una fecha de caducidad, que puede oscilar desde el tiempo que dure la sesión hasta una fecha futura especificada, a partir de la cual dejan de ser operativas.

Ingredientes de las cookies

Vamos a examinar a continuación la lista de ingredientes de una cookie. Tomaremos como ejemplo la cookie recomendada por el chef, la de Netscape.

Cada cookie representa una pequeña porción de información con una fecha de caducidad opcional, que se añade al fichero o directorio de cookies con el siguiente formato:

nombre = valor; expires = fechaCaducidad;

donde nombre es el nombre del dato almacenado, y valor representa su valor. La fecha de caducidad es un parámetro opcional que indica el tiempo que se conservará la cookie. Si no se especifica el valor de expires, la cookie caduca cuando el usuario sale de la sesión en curso con el navegador. Por consiguiente, el navegador conservará y recuperará la cookie sólo si su fecha de caducidad aún no ha expirado.

La caja de las cookies

Las cookies no las escribe el servidor, sino que es el propio navegador del cliente quien almacena la cookie en su disco duro.

Dónde se esconden

Veamos varias instrucciones para distintos sistemas operativos que nos permitirán rastrearlo:

Win 3.x

En el Administrador de archivos, en Archivo, selecciona Buscar y en la ventanita a tal efecto escribe cookies.txt

Win95 o WinNT

Pulsa Inicio, selecciona Buscar y luego Archivos o carpetas, escribe cookies.txt

Unix

Escribe en la línea de comandos:

find . −name cookies

Ahí tenemos dónde se almacenan las cookies con Netscape. Si se usa Microsoft Internet Explorer, hay que buscar en el directorio Win95 o WinNT, en el directorio llamado Cookies.

Usos de las cookies

¿Quién no ha pensado alguna vez en acceder a un sitio y encontrarlo personalizado a nuestro gusto? ¿A quién no le gustaría cuando se conecta a su librería virtual que le avisen de las novedades sobre aquellas materias que más le interesan? ¿A cuánta gente le parece muy complicado tener que teclear su nombre y contraseña cada vez que se conecta a un sitio? . Personalización, ésa es la palabra clave. Internet constituye una fantástica herramienta para crear presentaciones con el potencial de llegar a cualquier persona en cualquier lugar del mundo. Aunque la idea es muy atractiva, en la práctica ocurre que la información presentada en las páginas se torna impersonal. Es algo así como comprar un CD−ROM por el cual puedes navegar, incluso admirar animaciones y escuchar sonidos y música, pero que es igual para todo el mundo, y como todos sabemos, las mismas cosas no nos interesan a todos por igual. Lo que realmente nos gusta son los productos a nuestra medida, confeccionados especialmente para nosotros.

Usos bien vistos

Personalización de las páginas

A menudo se nos presenta la posibilidad de elegir entre navegar con o sin frames. A veces nos dan a elegir incluso el color del fondo o el tipo de letra. Toda esta información queda almacenada en una cookie, para que en visitas posteriores las páginas aparezcan a nuestro gusto, sin el engorro de ir apretando botones de configuración.

Idioma

Nos hemos topado más de una vez con páginas que nos ofrecen la posibilidad de elegir entre varios idiomas. Pues bien, si la primera vez que me conecto y elijo un idioma determinado, esta información se almacena en una cookie, las próximas veces que acceda a esas páginas, el texto aparecerá en el idioma seleccionado.

Tiendas electrónicas

Se han desarrollado sistemas de venta que almacenan en una cookie los gustos del usuario basándose en las páginas visitadas cuando accede para efectuar sus pedidos. Así, en lo sucesivo, cuando se conecte de nuevo, se le puede informar de las últimas novedades en aquellos artículos de su preferencia.

Carritos de la compra

Permiten recordar los artículos que un cliente va adquiriendo a medida que se mueve por las páginas del catálogo, como si los estuviera cargando en un carrito de la compra virtual, de manera que no tenga que ir pagándolos uno a uno, sino pagarlos todos de una vez cuando vaya a la página de pago.

Usos no tan bien vistos

Seguimiento de las visitas a un Web

He aquí una aplicación controvertida. Su objetivo es mantener un historial de las páginas visitadas por los usuarios dentro del servidor con el fin de conocer cuáles son las páginas menos visitadas, páginas a las que llega la gente pero de las que luego no sabe salir o de las que salen por falta de interés. También permiten recabar registros más exactos sobre el número de visitantes a una página, ya que las cookies permiten diferenciar 30 personas distintas visitando un sitio de una misma persona pulsando 30 veces el botón de recargar. Sin embargo, muchos piensan que se trata de una violación de la intimidad.

Carteles publicitarios

Muchas páginas muestran distintos anuncios o espacios publicitarios (banners) cada vez que nos conectamos a ellas. La forma de hacerlo es guardar en una cookie el identificador del último anuncio que nos han mostrado, de manera que la cada vez que nos conectemos nos presenten uno distinto.

Marketing personalizado

Se trata de la aplicación con fines comerciales más extendida. Las cookies se pueden emplear para construir un perfil de usuario con los lugares visitados, los anuncios (banners) que se han seguido, los productos comprados, etc. Esta información es posteriormente usada para enviarle anuncios que ellos creen le pueden interesar, así como para variar los anuncios mostrados (ver párrafo anterior). Ahora bien, ¿y si la compañía vende esta información a terceros? La polémica está servida.

Almacenamiento de nombre y contraseña

Todos hemos visitado sitios en los que nos piden nombre y contraseña para poder acceder a su contenido. Algunos de estos sitios además almacenan estos datos en una cookie que se guarda en el disco duro del usuario. De esta forma, la siguiente vez que acceda no se le volverá a pedir su nombre y contraseña. Si bien ningún otro servidor puede acceder a esta información, cualquier usuario accediendo físicamente al ordenador puede leer la cookie que contiene estos datos. Por ello, conviene almacenarlos cifrados, y también que caduquen al poco tiempo, días o incluso horas.

Almacenamiento de información sensible

Aunque parezca mentira, existen sitios que almacenan nuestro número de tarjeta en una cookie, para que en futuras transacciones comerciales con ellos no tengamos que introducirlo.

Alternativas a las cookies

Como queda dicho, la razón de ser de las cookies es almacenar el estado de la sesión entre peticiones sucesivas, puesto que el protocolo HTTP es sin estado. No obstante, existen por lo menos otros dos métodos que ya eran usados mucho antes de que aparecieran las cookies, a saber, transmitir datos del estado de la sesión a través de campos ocultos en los formularios CGI y añadir datos del estado al final de un URL.

Ataque y Defensa (Web seguro)

Para localizar una máquina en Internet es necesario conocer la dirección IP asignadas por el ISP (Proveedor de Servicios Internet). Aunque la dirección IP identifica a una máquina no proporciona una vía de acesso a ellas.

Para tener acceso es necesario encontar un puerto abierto. Por ejemplo, en el caso del acceso Web, por lo general, es necesario el puerto 8080 o 80 más popularmente conocido y en el caso del acceso FTP (Protocolo de transferencia de archivos) necesitamos el puerto 21.

Por lo tanto, una vez conocido la dirección IP, es necesario escanear los puertos de la máquina cuya dirección conocemos. Para este motivo, es importante, adquirir las herramientas necesarias conocidas como escaneadores de puertos. Estos programas varían de formato pero tienen como objetivo el mismo fin.

Otro método de apertura de puertos es enviar al usuario un programa que despliegue un "Caballo de Troya" o "Troyano". Reproduciendo la táctica de los antiguos griegos, los caballos de Troya actúan bajo una apariencia benigna dañando o modificando secretamente el sistema. En algunos caso, se pueden encubrir bajo un anexo o attachment del correo electrónico.

Uno de los troyanos más conocidos es el "Back Orifice" cuyo nombre parodia al nombre del software de administración de redes de Microsoft: BackOffice. El objetivo del Back Orifice es abrir un puerto en la computadora para obtener el control a distancia de la máquina. Otros Troyanos de igual importancia existentes pero de inferior reputación son UMG32.exe y el Sub Seven que ocasionan el mismo efecto que el Back Orifice.

Planteamiento de la Defensa

Ante lo anterior, entonces, debemos planificar una estrategia de defensa. La decisión de verificar cada uno de los puertos abiertos por los programas, resultaría tedioso e infructuoso. Por lo tanto, esta tarea debe realizarse mediante programas o hardware encargado de verificar la entrada y salida de cada uno de los puertos. Estos programas o hardware denominados "firewalls" o "cortafuegos" realizan la laboriosa misión antes descrita.

También es necesario implementar políticas en los sistemas operativos que ofrezcan los servicios de Web o FTP. En caso de un servidor tipo basado en tecnología NT 4.0 la configuración de apertura o clausura de los puertos es bastante flexible; es posible realizarla desde la misma ventana de configuración del protocolo TCP/IP. Sin embargo, debe utilizarla con cautela pues la inexperiencia del administrador puede dejar sin comunicación al servidor.

Otros métodos de defensa es la implementación de un cortafuego y detrás de estos el montaje en cascada de proxies que controlan el tráfico interno de la red. Prácticamente la entrada al servidor mediante una zona militarizada es prácticamente nula.

Uno de los más grandes problemas a la hora de realizar una política de seguridad de nuestros equipos y redes internos ante Internet y la amenaza foránea es que también existe la amenaza interna. Ante esto, es necesario implementar políticas de grupos que limiten los permisos y expliciten los mismos con tal de establecer reglas claras.

Conclusión

Actualmente, el desarrollo de Internet involucra un aspecto fundamental denominado Seguridad por el que

muchas de las empresas que implementan comercio electrónico han gastado gran parte de sus recursos en hacer de esta una piedra angular de toda su estructura.

Debido a esto, antes de comenzar la implementación de cualquier sitio Web es necesario conocer, las rutinas de seguridad mínimas que deben poseer tanto nuestro servidor como nuestras aplicaciones.

Sin ellas, cualquier intento de desarrollo es absolutamente vulnerable a los frecuentes ataques por parte de piratas informáticos o simples ataques benignos por parte de curiosos.

En los próximos años, los métodos de seguridad aumentaran para dar paso a una sensación de seguridad mayor de la que hoy en DIA existe.

Bibliografía

FARLEY, Marc *Guía Lan Times de seguridad e integridad de datos* Ed. McGraw−Hill, Madrid España. Pp 199−245.

PC Magazine, Vol. 113 N° 9, Septiembre 2000

Internet:

http://soporte.udg.mx/websoporte/seguridad/seguridad.html

http://cdec.unican.es/libro/

29