ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

"¿QUÉ OCURRE EN LA ACTUALIDAD CON LA SEGURIDAD? INVESTIGA"

AUTORÍA
MARÍA CATALÁ CARBONERO

TEMÁTICA
SEGURIDAD, REDES

ETAPA
CICLO SUPERIOR DE INFORMÁTICA Y PROFESORADO

Resumen

La seguridad en los sistemas en red es un tema actual y con vistas de futuro en las empresas, en la vida cotidiana y en la educación. Hoy en día necesitamos certificados para entrar en páginas web, contraseñas para acceder a nuestro correo electrónico, firmas digitales para hacer operaciones en nuestro banco, etc. En este artículo se verán las técnicas y los sistemas de protección actuales y como han ido evolucionando a través de la historia.

Palabras clave

Criptografía, cifrar, descifrar, clave pública, clave privada, firma digital.

1. INTRODUCCIÓN

La seguridad en sistemas en red consiste en proteger los datos y los programas contra fallos del equipo, errores de los programas o de los usuarios, o causas humanas o naturales, bien sean accidentales o en red.

La seguridad de un sistema en red, además deberá contemplar, al menos, las siguientes medidas básicas:

- Protección de la información
  - Realizar copias de seguridad de los datos y del software del sistema.
  - Disponer de equipos de reserva, por si falla alguno de los utilizados.
  - Control de acceso a los usuarios del sistema.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

- Protección de los equipos y sus instalaciones
  - Control de acceso a la zona donde se encuentran los equipos.
  - Control ambiental, es decir, protegerlo de la suciedad: polvo, humo, líquidos, resto de comidas.
  - Planificación para evitar accidentes.
  - Prevención contra incendios, agua, temperaturas extremas, etc.

2. TIPOS DE ATAQUES A LA SEGURIDAD DE UN SISTEMA EN RED

Se pueden clasificar los ataques a la red en dos tipos, en función de si se altera o no el contenido de la información de la misma.

2.1. Ataques Pasivos

Consisten en la obtención no autorizada de la información. Distinguimos los siguientes tipos:

- Divulgación del contenido de un mensaje
- Análisis del tráfico para interceptar señales y obtener datos sin autorización.

2.2. Ataques Activos

Consisten en la eliminación o alteración de datos de la red. Se subdividen en cuatro categorías:

- *Enmascaramiento*: tiene lugar cuando una entidad es suplantada por otra entidad diferente.
- *Repetición*: supone la captura pasiva de unidades de datos y su retransmisión de forma iterativa.
- *Modificación del mensaje*: significa que alguna porción de un mensaje legítimo se altera, o que el mensaje se retrasa o se desordena.
- *Denegación de un servicio*: impide el uso normal de los recursos de la red, por ejemplo, saturando algún servicio de comunicación.

3. OBJETIVOS DE UN SISTEMA DE SEGURIDAD

Los objetivos básicos que debe cubrir la seguridad de un sistema en red son:

- Minimizar la probabilidad de una intrusión, proporcionando dispositivos y procedimientos de protección.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

- Detectar cualquier intrusión tan pronto como sea posible.
- Identificar la información objeto del ataque y obtener la información de control y estado necesario para recuperarse del ataque.

4. SERVICIOS DE SEGURIDAD

Los sistemas seguros en red deben de proporcionar los siguientes servicios de seguridad:

- *Confidencialidad*: Protección de los datos transmitidos contra personas no autorizadas.
- *Integridad*: Seguridad de que los datos recibidos no contienen duplicaciones, inserciones, modificaciones o sustituciones.
- *Verificación de identidad de pareja*: Identificación de entidades remotas, eliminando la posibilidad de que se repitan secuencias de verificación previas.
- *Control de acceso*: limitación y control del acceso a ordenadores principales mediante enlaces de comunicaciones.
- *Seguridad en el flujo del tráfico*: Modelos de enmascaramiento u ocultación de tráfico.
- *No rechazo*: Seguridad de que el receptor de los datos no negará que los ha recibido, n el remitente que los ha enviado.
- *Verificación del origen de los datos*: Seguridad de que la fuente de los datos es requerida.

5. TÉCNICAS Y SISTEMAS DE PROTECCIÓN

Estas técnicas son una serie de precauciones para reducir la probabilidad de fallos en la seguridad de las comunicaciones.

Las técnicas y métodos son muy variados pero pueden clasificarse según utilicen técnicas centralizadas o distribuidas.

La *técnica distribuida* puede ser de una subred dentro de una red, o de un ordenador dentro de una subred. Cada uno se encarga de proteger su parte de agresiones e incursiones externas. Esto se conoce normalmente como blindaje de redes o de ordenadores, y engloba a los métodos más utilizados, entre ellos el cortafuegos.

En la técnica centralizada se fijan unos puntos de control para detectar paquetes agresivos o intrusos, incluso actuando como cebo de éstos. También se actúa de forma inversa, comportándose como un

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

intruso (hacker) para descubrir los puntos débiles del sistema, y corregir el problema antes de que alguien lo descubra.

Actividad 1: La encriptación es uno de los métodos de seguridad más usados para el envío de datos. Se podría especificar un trabajo en grupo en el que cada grupo especifique en un *power-point* la importancia de este concepto, teniendo especial atención a los siguientes puntos:

¿Qué es la encriptación?

Tipos: clave simétrica y asimétrica

Principales problemas de la encriptación

5.1. Algunos métodos de protección

5.1.1 Defensas contra la intervención de líneas

Allí donde exista una ruta de comunicaciones bajo control completo de los usuarios, se pueden realizar precauciones como:

- Instalar filtros de paso bajo en los cables principales y en los cables de señalización eléctrica conectados al equipo.
- Instalar equipos en un área que no tenga cables, tuberías conductoras o teléfono.
- Realizar una inspección visual regular del camino completo de señal.

5.1.2 Códigos de identificación

Se calculan y añaden al mensaje en el dispositivo de emisión, y se comprueban en los dispositivos de recepción. Éstos pueden utilizarse para prevenir la inserción de falsos mensajes por el intruso, y para la repetición de un mensaje procedente de una secuenciación previa.

5.1.3 Ordenación de los mensajes

Es usual utilizar un número de secuencia de entrada para todos los mensajes enviados desde el terminal y un número de secuencia de salida para todos los mensajes que se envían al terminal.

5.1.4 Procedimientos operacionales y auditoria

Las auditorias permiten reconstruir la secuencia de acciones tras un intento de violación de seguridad o de un fallo del sistema.

5.1.5 Protección de puertos

Dentro de esta protección nos encontramos con:

- Uso de contraseñas para el acceso de los usuarios a los puertos de un ordenador en sistemas de acceso a terminales remotos.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

- Dispositivos de protección de puertos

6. SISTEMAS DE PROTECCIÓN ESTÁNDARES

Actualmente casi todos los estándares existentes dedicados a la seguridad en redes, se basan en los principios de la criptografía.

6.1. Criptografía

Todos los sistemas criptográficos modernos se basan en el principio de Kerkhoff, que afirma que todos los algoritmos de cifrado y descifrado deben ser públicos y conocidos por todos, por tanto lo único secreto es la clave del algoritmo.

La encriptación por tanto consiste en codificar un mensaje con el fin de que ninguna persona no deseada lea su contenido.

6.2. Algoritmos Criptográficos

6.2.1 Criptografía clave simétrica

Se emplea la misma clave para codificar y decodificar el mensaje. En la actualidad los algoritmos más utilizados son DES (Estándar de Encriptación de Datos), triple DES, y el AES (Estándar de Encriptación Avanzado).

6.2.2 Criptografía clave compartida

Varios usuarios autorizados tienen partes de la clave, y el proceso de descifrado sólo se consigue si se reúnen un número mínimo de ellos para recomponer entre todos la clave.

6.2.3 Criptografía clave maestra o jerárquica

Una empresa u organización posee una llave maestra de la que se derivan las claves de los usuarios utilizando su identidad, por ejemplo su DNI.

6.2.4 Criptografía clave pública o asimétrica

Es un sistema en el que el método de encriptación es públicamente conocido, pero el desencriptado es solo conocido por el propietario. El algoritmo principal de clave pública es RSA.

6.3. Estándares de Seguridad en redes

6.3.1 Firmas digitales

Es un mecanismo que busca un efecto similar al de las firmas manuscritas. Sus objetivos son

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

- Identificación: certifica que el emisor es quién dice ser.
- Compromiso: certifica que el emisor fue el autor de la operación.

Este estándar utiliza algoritmos de clave simétrica (firmas de clave simétrica) y de clave pública (Firmas de clave pública).

6.3.2 Certificados digitales

Consiste en distribuir claves públicas para aquellos usuarios que deseen una comunicación segura en la red.

El estándar para certificados, aprobado por la ITU es el X.509, y es muy utilizada en Internet. En la actualidad, organismos oficiales distribuyen este tipo de certificados para realizar trámites a través de Internet (hacienda, Seguridad Social, etc.)

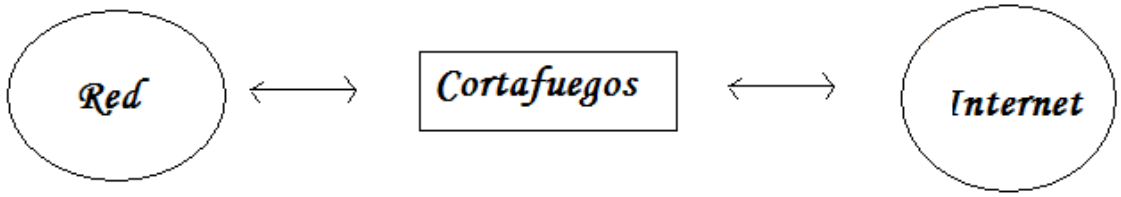
6.3.3 IPsec (IP seguro)

Es un estándar descrito en los RFCs 2401, 2024 y 2406 entre otros. Ofrece los servicios de confidencialidad, integridad de datos, y protección contra ataques de repetición. Y se basan en la criptografía simétrica.

6.3.4 Cortafuegos (Firewalls)

Se implementa para proteger los ordenadores de la red, intentando evitar la intrusión en los equipos, para extraer información sin autorización, y la infiltración de información no deseada como por ejemplo un virus.

Se trata de filtrar el tráfico de información entrante y saliente de una red perteneciente a una organización (red interna), hacia otra red externa (por ejemplo Internet), pudiendo restringir, y hasta, interrumpir una conexión.



Existen varios niveles de cortafuegos:

- *Cortafuegos filtradores de paquetes*: son enrutadores especiales que filtran ciertos paquetes, actuando de firewalls de bajo nivel.
- *Cortafuegos a nivel de circuitos*: pueden ser un ordenador que actúa a modo de gateway filtrando paquetes, pero pudiendo añadir funciones avanzadas de autentificación.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

- *Cortafuegos a nivel de aplicación*: consiste en introducir una minired virtual, entre la red interna e Internet, con un host que controla todo lo que entra y sale, pudiendo pedir contraseñas y autentificación.

Actividad 2: Existen muchas estrategias de seguridad, tal y como se ha explicado anteriormente, sería conveniente intentar motivar al alumnado especificando un trabajo en el que busquen información sobre las distintas técnicas de cortafuegos que existen actualmente, y que tanto se utilizan tanto en la vida cotidiana como laboral

6.3.5 Redes privadas virtuales, IP tunneling

Son redes superpuestas sobre redes públicas, pero manteniendo muchas propiedades de las redes privadas.

Se llaman virtuales porque no existen realmente. Se trata de crear una red aparente con nodos que realmente no forman parte de la misma red física, de manera que las aplicaciones "crean" que estos nodos están dentro de una misma red, pudiendo así proporcionarles servicios y privilegios que correspondan.

Un ejemplo sería el acceso a una base de datos de una universidad. Si desde nuestro domicilio nos conectamos a esta red (mediante VPN) el sistema nos integrará en la red de la universidad, a pesar de no formar conexión física en dicha subred, pudiendo acceder así a estas bases de datos restringidas.

6.3.6 Autentificación

Es una técnica que consiste en demostrar la veracidad de un proceso remoto para asegurarse su identidad. Se pretende evitar la presencia de intrusos en la red.

Si dos equipos establecen una sesión, deben autentificarse entre sí, y si es necesario, establecer una clave de sesión compartida.

Existen varios protocolos de autentificación basados en algoritmos de clave secreta compartida (Diffie-Helman y Kerberos), y también de clave pública.

6.3.7 Seguridad Inalámbrica

Las redes inalámbricas son más inseguras que las cableadas, porque la transmisión por radio es fácilmente accesible por los equipos ajenos.

Para resolver este problema, el estándar 802.11 estableció un protocolo a nivel de enlace llamado WEB (Privacidad Inalámbrica Equivalente) basado en establecer una clave entre el ordenador y la estación base. Se ha demostrado que este protocolo no es eficiente.

El IEEE informó recientemente que el próximo estándar de redes inalámbricas 802.11i tendrá como objetivo prioritario mejorar la seguridad.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 23 – OCTUBRE DE 2009

Actividad 3: Como última actividad, sería muy interesante que el alumnado realizara una comparación entre los antivirus más conocidos en el mercado: Norton, Bitdefender, Panda, Nod32, Kaspersky, Avast, McAfee, etc. Tendrán que prestar mucha atención al *precio y servicios* que ofrece cada uno de ellos.

7. BIBLIOGRAFÍA

- Tanembaum, A. (2003). *Redes de Computadoras, 4ª Edición*: Prentice Hall
- Stallings, W. (2004). *Redes e Internet de Alta Velocidad. Rendimiento y Calidad de Servicio, 2ª Edición*: Prentice-Hall

Autoría

- María Catalá Carbonero
- IES Florencio-Pintado, Peñarroya-Pueblonuevo, Córdoba
- mcata44@hotmail.com