Preparador Informática

www.preparadorinformatica.com

TEMA 72 INFORMÁTICA

LA SEGURIDAD EN SISTEMAS EN RED. SERVICIOS DE SEGURIDAD. TÉCNICAS Y SISTEMAS DE PROTECCIÓN. ESTÁNDARES

TEMA 63. S.A.I.

SEGURIDAD DE LOS SISTEMAS EN RED

TEMA 72 INF: LA SEGURIDAD EN SISTEMAS EN RED. SERVICIOS DE SEGURIDAD. TÉCNICAS Y SISTEMAS DE PROTECCIÓN. ESTÁNDARES.

TEMA 63 SAI: SEGURIDAD DE LOS SISTEMAS EN RED.

1. INTRODUCCIÓN

Desde los inicios de Internet y hasta finales de los años 90, casi toda la información que circulaba por Internet no utilizaba ningún tipo de cifrado. Posteriormente, su expansión hacia el público en general hizo que el número de usuarios creciera exponencialmente y también la proliferación de ataques realizados contra empresas y particulares, obligando a pensar decididamente en el concepto de seguridad de los sistemas.

En la seguridad en los sistemas en red podemos distinguir entre la seguridad física y la seguridad lógica. La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware. Las amenazas físicas pueden ser provocadas por el hombre, ya sea de forma voluntaria o involuntaria, o por la acción incontrolada de la naturaleza. Por otra parte, la seguridad lógica, que será en la que nos centraremos a lo largo del tema, consiste en la aplicación de procedimientos que protejan el acceso a los datos y a la información de las amenazas lógicas.

Podemos clasificar los posibles ataques lógicos en pasivos y activos. En los ataques de tipo pasivo el atacante no altera la comunicación, tan sólo tiene acceso a ella. De esta forma puede saber qué información circula por el canal, a qué horas, la frecuencia y entre qué personas. Este tipo de ataque es más difícil de detectar ya que no aparece ningún signo que nos pueda advertir de que estamos siendo atacados. Por el contrario, en los ataques activos el atacante modifica el flujo de datos transmitidos o incluso crea uno falso, permitiendo incluso la suplantación de un usuario legítimo.

El presente tema está dedicado a estudiar la importancia de la seguridad de los sistemas en red describiendo para ello mecanismos de seguridad como son las técnicas criptográficas, protocolos de seguridad como SSL, TLS, IPSec, mecanismos de seguridad a nivel de red, entendido como conjunto de elementos físicos (red, servidores, routers, cortafuegos, etc.) y lógicos (protocolos, técnicas, servicios, etc.)

2. LA SEGURIDAD EN SISTEMAS EN RED

El sistema de seguridad requerido por una organización variará dependiendo de una serie de factores, entre los que pueden destacarse los siguientes:

- Localización geográfica de los usuarios.
- Topología de la red de comunicaciones.
- Instalaciones o salas donde residen los equipos físicos.
- Equipo físico que soporta el SI.
- Configuración del equipo lógico básico.
- Tipo y estructura de las bases de datos.
- Forma de almacenamiento de los datos.
- Número y complejidad de los procesos a realizar.

2.1. SERVICIOS DE SEGURIDAD

Las políticas de seguridad de los sistemas en red tienen como objetivo ofrecer servicios de seguridad que salvaguarden las comunicaciones ante posibles ataques, para lo cual se emplean una serie de protocolos de seguridad.

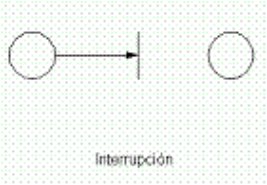
Los servicios de seguridad más importantes son:

- **Autenticación:** propiedad que garantiza la identificación fidedigna de los usuarios en un sistema.
- **Confidencialidad**: requiere que la información sea accesible únicamente por las entidades autorizadas.
- **Integridad**: requiere que la información sólo pueda ser modificada por las entidades autorizadas.
- **Disponibilidad**: requiere que los recursos del sistema estén disponibles para las entidades autorizadas cuando los necesiten.
- **No repudio**: ofrece protección a un usuario frente a otro que niegue posteriormente que se realizó cierta comunicación (en origen y destino).

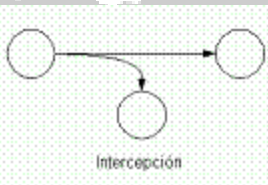
2.2. TIPOS DE AMENAZAS

Las amenazas pueden ser clasificadas principalmente en cuatro grupos distintos:

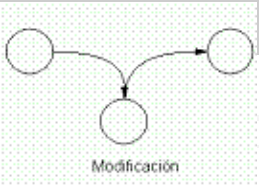
- **Interrupción:** La interrupción es una amenaza en la que un recurso del sistema es destruido o deja de estar disponible. Ejemplo: Ransoware



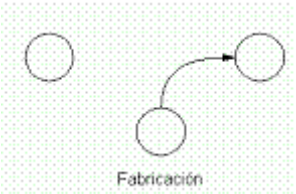
- **Intercepción:** La intercepción es una amenaza en la que una entidad no autorizada consigue acceso a un recurso. Ejemplo: Keyloggers



- **Modificación:** La modificación es una amenaza en la que una entidad no autorizada consigue acceder a un recurso y manipularlo.



- **Fabricación:** La fabricación es una amenaza en la que una entidad no autorizada inserta objetos falsificados en el sistema. Ej: Hijacking.



2.3. TÉCNICAS Y SISTEMAS DE PROTECCIÓN

2.3.1. TÉCNICAS CRIPTOGRÁFICAS

El cifrado transforma una información (texto claro) en otra ininteligible (texto cifrado), con el objetivo de garantizar su confidencialidad.

Básicamente se distinguen dos sistemas de cifrado: **cifrado simétrico y cifrado asimétrico.**

2.3.1.1. CRIPTOGRAFÍA SIMÉTRICA

Un criptosistema con cifrado simétrico se caracteriza por utilizar la misma clave en las transformaciones de cifrado y descifrado por el emisor y el receptor. La seguridad del sistema depende de que nadie más conozca la clave. La clave debe ser secreta para cualquier otro individuo o entidad distintos del emisor y el receptor.

Ejemplos de técnicas criptográficas simétricas: DES, TDES, IDEA, AES, Blowfish, RC4, RC5, RC6, SEAL, SAFER.

2.3.1.2. CRIPTOGRAFÍA ASIMÉTRICA

Un criptosistema con cifrado asimétrico se caracteriza porque el emisor y receptor tienen cada uno una pareja de claves (clave pública y clave privada). La clave privada debe mantenerse en secreto por el emisor y la clave pública se distribuye a todos los posibles destinatarios. Lo que cifra una clave privada solo puede ser descifrado por la clave pública correspondiente y viceversa. La clave privada no puede deducirse de la pública por lo que no hay peligro en transmitir las claves públicas por la red. De este modo:

- Si el emisor cifra con la clave pública del receptor, entonces el receptor descifra con su clave privada.
- Si el emisor cifra con su clave privada, entonces el receptor descifra con la clave pública del emisor.

Ejemplos de técnicas criptográficas simétricas: RSA, DSA, Diffie-Hellman.

2.3.1.3. ALGORITMOS HASH

Un algoritmo hash es un algoritmo unidireccional que calcula a partir de una cadena de bits de longitud arbitraria otra de longitud fija. Los algoritmos hash se aplican a unos datos para obtener un resumen o huella digital que se utiliza en la firma digital. Se utiliza para verificar la integridad de los datos.

Ejemplos: SHA-1, MD5, RIPEMD-160

2.3.2. PROTOCOLOS DE SEGURIDAD

2.3.2.1. SECURE SOCKET LAYER (SSL)

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket, de forma transparente al usuario y a las aplicaciones que lo usan.

El objetivo principal del protocolo SSL es proporcionar privacidad y fiabilidad entre dos aplicaciones que se comunican.

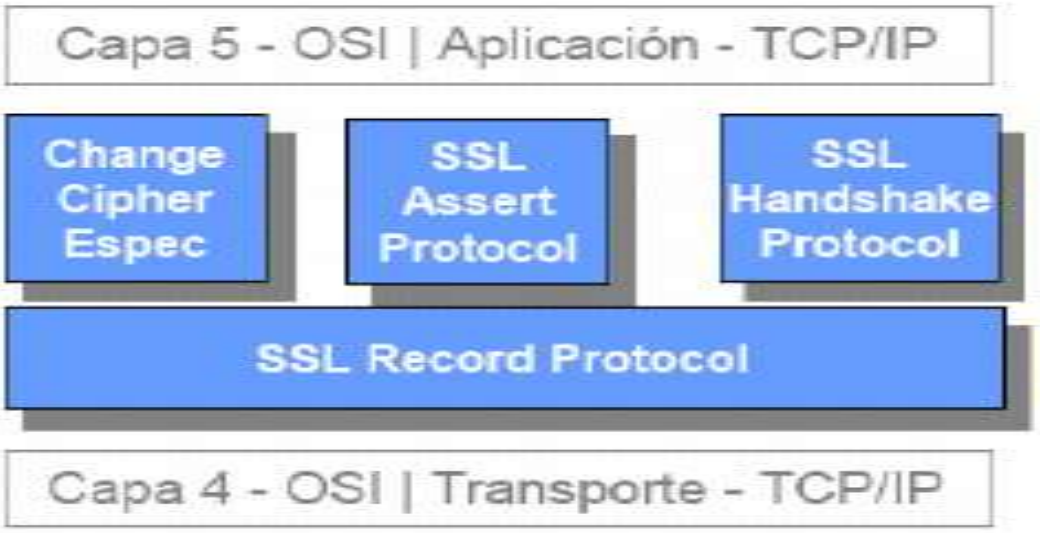
El protocolo está compuesto por dos capas:

A) Capa inferior

- **SSL Record Protocol**: se utiliza para la encapsulación de diversos protocolos de nivel superior pertenecientes a SSL

B) Capa superior

- **SSL Handshake Protocol**: permite al cliente y servidor autenticarse mutuamente y negociar un algoritmo de cifrado y claves criptográficas antes de que el protocolo de aplicación transmita o reciba su primer byte de datos
- **SSL Change Cipher Spec Protocol**: permite enviar señales de cambios en las estrategias de cifrado.
- **SSL Alert Protocol**: se encarga de enviar un mensaje cuando se produce un posible error.



2.3.2.2. TRANSPORT LAYER SECURITY (TLS)

El protocolo TLS es una evolución del protocolo SSL dado que está basado en éste último y funciona de manera muy similar. TLS fue definido en 1999 y actualizado en el RFC 5246 (2008) y en RFC 6176 (2011)

Desde el punto de vista de su implementación en los modelos de referencia OSI y TCP/IP, SSL y TLS se introduce como una especie de capa adicional, situada entre la capa de Aplicación y la capa de Transporte.

Existen varios protocolos de aplicación que utilizan SSL/TLS para ofrecer seguridad a la información intercambiada. Por ejemplo, el protocolo https (http sobre SSL/TSL) tiene asignado el puerto 443.

2.3.2.3. IPSEC

IPSec proporciona servicios de seguridad basados en criptografía a la capa IP y a todos los protocolos superiores basados en IP.

El conjunto de servicios de seguridad ofrecidos incluye: control de acceso, integridad sin conexión, autenticación del origen de los datos, protección antireplay y confidencialidad del flujo de tráfico (cifrado). Estos servicios se implementan en la capa IP, y ofrecen protección para este nivel y/o los niveles superiores. Para ello, combina tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y

certificados digitales X509v3. Los servicios se proporcionan en la capa IP, y pueden ser utilizados por cualquier protocolo de capa superior, por ejemplo, TCP, UDP, ICMP, BGP, etc.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad que proporcionan mecanismos de seguridad para proteger tráfico IP:
    - IP Authentication Header (AH)
    - IP Encapsulating Security Payload (ESP).
- Un protocolo de gestión de claves:
    - Internet Key Exchange (IKE): permite a dos nodos negociar las claves y los parámetros necesarios para establecer una conexión AH o ESP.

Estos protocolos soportan dos modos de uso: modo transporte y modo túnel.

1. **Modo transporte.** En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

2. **Modo túnel**. En este modo el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

2.3.3. CORTAFUEGOS

Un cortafuegos es una combinación de técnicas, políticas de seguridad y tecnologías (hardware y software) encaminadas a proporcionar seguridad en la red controlando el tráfico que circula.

Como norma general en las organizaciones suelen existir diferentes niveles de cortafuegos para incrementar la seguridad, separando así las distintas redes y dificultando los posibles ataques.

2.3.3.1. FUNCIONES DE UN CORTAFUEGOS

Entre las funciones típicas de un cortafuego están:

- Controlar, permitiendo o denegando, los accesos desde la red local hacia el exterior y viceversa.
- Filtrar los paquetes que circulan, de modo que sólo los servicios permitidos puedan pasar
- Traducción de direcciones (NAT)
- Monitorizar el tráfico, supervisando destino, origen y cantidad de información recibida y/o enviada
- Filtrado de contenidos.
- Prevención de intrusiones.

2.3.3.2. TIPOS DE CORTAFUEGOS

Existen distintos tipos de cortafuegos, dependiendo de las funcionalidades que ofrecen y de las capas OSI en las que actúan.

A continuación, se presenta una clasificación de los mismos:

A) FILTRADO DE PAQUETES

Se utilizan routers con filtros y reglas basadas en políticas de control de acceso. El router es el encargado de filtrar los paquetes, en base a cualquiera de los siguientes criterios:

- ✓ Protocolos utilizados
- ✓ Dirección IP de origen y de destino
- ✓ Puerto TCP – UDP de origen y de destino

Este tipo de cortafuegos trabaja en los niveles de transporte y de red del modelo OSI. Tienen la ventaja de ser económicos y son transparentes para los usuarios conectados a la red. Desventajas:

- ✓ No protegen las capas superiores a nivel OSI
- ✓ No soportan políticas de seguridad complejas, como autenticación de usuarios y control de accesos con horarios prefijados.

B) PROXY

Se trata de un software de aplicación encargado de filtrar las conexiones. Estas aplicaciones son conocidas como servidores proxy, y la máquina donde se ejecuta recibe el nombre de gateway de aplicación o host bastión. El proxy actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario solicita un servicio, lo hace a través del proxy. Su función es la de analizar el tráfico de red en busca de contenidos que violen la seguridad de la misma.

C) INSPECCIÓN DE PAQUETES (DETECCIÓN DE INTRUSOS)

Este tipo de cortafuegos se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la **capa de red** hasta la de **aplicaciones**. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

2.3.4. REDES PRIVADAS VIRTUALES (VPN)

2.3.4.1. INFRAESTRUCTURA VPN

Una Red Privada Virtual conecta los componentes y recursos de una red sobre otra, mediante la implementación de un túnel a través de Internet, de manera que los participantes del túnel se beneficien de las condiciones de seguridad que normalmente se ofrecen en una red privada.

2.3.4.2. TUNNELING

Se denomina tunneling al método que permite usar la infraestructura de Internet para transferir datos en forma segura desde una red sobre otra, mediante un camino lógico (túnel) a través del cual los paquetes viajan encapsulados a través de la red.

Los datos a ser transferidos pueden ser tramas o paquetes de otro protocolo. En lugar de enviar la trama tal como fue generada por el nodo origen, el protocolo de "tunneling" encapsula la trama en otro encabezado adicional, el cual provee información de enrutamiento que le permite a los datos atravesar la red intermedia. De ese modo, los paquetes encapsulados son enrutados entre los extremos del túnel. Una vez que las tramas encapsuladas alcanzan su destino en la red, la trama es desencapsulada y entregada a su destino final. Se debe notar que "tunneling" es el proceso completo (encapsulado, transmisión, y desencapsulado de los paquetes).

Los protocolos PPPT y L2TP son protocolos de "tunneling" de Capa 2 que utilizan tramas como unidad de intercambio, encapsulándolas en una trama PPP ("Point-to-Point Protocol") para ser enviados a través de la red, mientras que el protocolo IPSec (estudiado anteriormente) es un protocolo de "tunneling" de Capa 3 que utiliza paquetes IP encapsulándolos con un encabezado IP adicional antes de enviarlo a través de la red IP.

Las principales implementaciones de túneles sobre VPNs en estos niveles están dadas por las propuestas cursadas (RFCs, Request for Comments) a la Internet Engineering Task Force (I.E.T.F.). Estas pueden agruparse según el nivel de protocolos que usen: Túnel de Capa 3 (tal como IPSec), y Túnel de Capa 2 (tal como L2TP).

3. ESTÁNDARES

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La serie de normas ISO/IEC 2700 permite a una organización que esté certificada con ella:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Etc.

4. CONCLUSIÓN

La información ha pasado a formar parte de la actividad cotidiana de empresas y particulares. Cuanto mayor es el valor de la información gestionada, más importante es asegurarla.

Por ello, resulta fundamental el aspecto de la seguridad de los sistemas en red estableciendo mecanismos para la prevención y reacción a incidentes de seguridad, con objeto de minimizar su probabilidad o su impacto en el caso de que se produzcan.

5. BIBLIOGRAFÍA

- Tanenbaum A. **Redes de computadores**. Editorial Pearson.
- Gómez, J. **Seguridad en sistemas operativos Windows y Linux.** Ed RaMa
- Costas J.: **Seguridad y alta disponibilidad**. Editorial Ra-Ma
- **Serie ISO/IEC 27000:** Estándares sobre Sistemas de Gestión de la Seguridad de la Información.
- www.incibe.es (Instituto Nacional de Ciberseguridad de España)
- www.ccn-cert.cni.es/ (Centro Criptológico Nacional)