MÓDULO 2 MF0964_3: DESARROLLO DE ELEMENTOS DE SOFTWARE PARA GESTIÓN DE SISTEMAS

UNIDAD 3 UF1288: DESARROLLO DE COMPONENTES SOFTWARE PARA SERVICIOS DE COMUNICACIONES

4 Seguridad en las comunicaciones

core networks

4 Seguridad en las comunicaciones

4.1 Introducción

core networks

Seguridad en las comunicaciones

La seguridad informática se extiende a las comunicaciones en red a través de las tres exigencias comunes a cualquier proceso:

- Secreto. Acceso a la información solo a los entes autorizados.
- Integridad. Acceso a la información solo por los entes autorizados.
- Disponibilidad. La información deberá estar siempre disponible a los entes autorizados.

4 Seguridad en las comunicaciones

4.2 Principios de seguridad en las comunicaciones

core networks

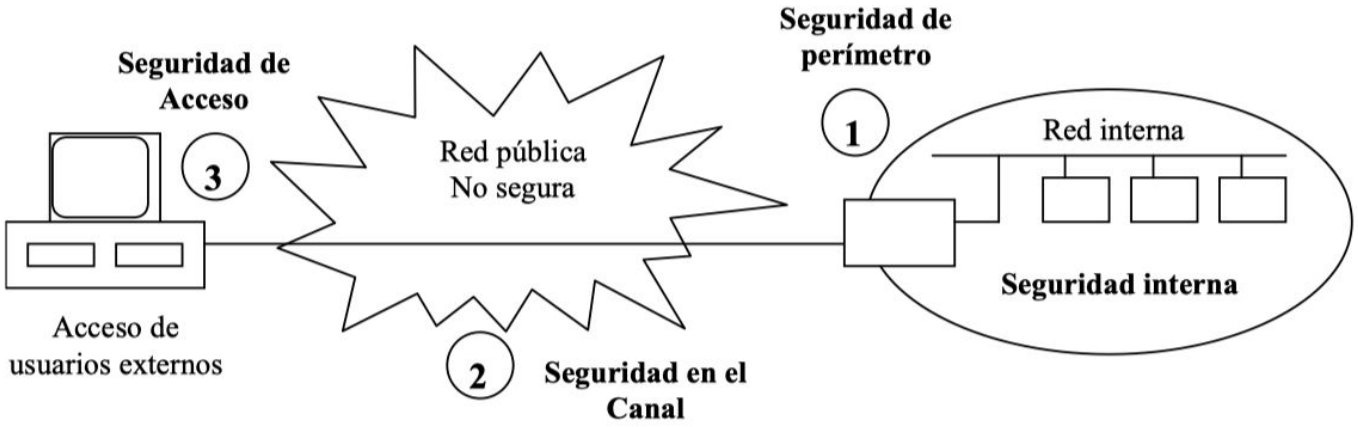
Principios de seguridad

Toda transacción segura por la red debe contemplar los aspectos de Autenticidad, Integridad, Confidencialidad y No Repudio:

- Seguridad de acceso.
- Seguridad en el canal.
- Seguridad de perímetro.

core networks

Principios de seguridad (II)



4 Seguridad en las comunicaciones

4.3 Herramientas para la gestión de la seguridad en red. Scanners

core networks

Scanners

4 Seguridad en las comunicaciones

4.4 Seguridad IP

core networks

Seguridad IP

TCP/IP es la identificación del grupo de protocolos de red basado en OSI que hacen posible la transferencia de datos en redes, entre equipos informáticos e internet. Las siglas TCP/IP hacen referencia a este grupo de protocolos:

- TCP es el Protocolo de Control de Transmisión que permite establecer una conexión y el intercambio de datos entre dos anfitriones. Este protocolo proporciona un transporte fiable de datos.
- IP o protocolo de internet, utiliza direcciones series de cuatro octetos con formato de punto decimal (como por ejemplo 75.4.160.25). Este protocolo lleva los datos a otras máquinas de la red.

4 Seguridad en las comunicaciones

4.5 Seguridad en el nivel de aplicación. El protocolo SSL

core networks

SSL

Secure Socket Layer es un sistema de protocolos de caracter general diseñado en 1994 por la empresa Nestcape Communcations Corporation, y está basado en la aplicación conjunta de criptografía simétrica, criptografía asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet.

De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se aprovecha la rapidez de operación, mientras que los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la confidencialidad en la transmisión de datos.

4 Seguridad en las comunicaciones

4.6 Seguridad en redes inalámbricas

core networks

Seguridad inalámbrica

Cifrado WPA. El cifrado WPA nació a partir de la necesidad de solucionar los problemas del cifrado WEP. Este sistema de cifrado ofrece una serie de variantes según la finalidad que se le vaya a dar:

- WPA-Personal: Utiliza un sistema de claves PSK o claves precompartidas donde el administrador especifica su propia contraseña y todos los usuarios se conectan a la red con ella, de manera que sea más fácil recordarla.
- RADIUS: Enfocado a empresas, este sistema de seguridad se basa en un servidor en el que los usuarios deben autenticarse con un usuario y una contraseña diferente para cada uno en vez de conectarse todos con una contraseña global.

Seguridad inalámbrica (II)

Cifrado WPA2. El cifrado WPA2 es la actualización del cifrado WPA y mejora tanto la seguridad como el rendimiento de este. Este sistema también cuenta con las variantes de claves personales PSK y sistemas RADIUS para la gestión de redes, aunque el cifrado es muy superior al de WPA.

4 Seguridad en las comunicaciones

4.7 Resumen

core networks

Resumen

- Comunicaciones en red.
- Modelos de programación en red.
- Modelo OSI y modelo TCP/IP.
- El nivel de enlace.
- El nivel de transporte.