Tema 5 – Seguridad en redes

1 Introducción

Se presentan distintas amenazas a la integridad, confidencialidad, autenticación y denegación de servicios.

Inicialmente, la IETF creó un grupo de trabajo, wts donde se crearon protocolos como SHTTP, mientras que la empresa Netscape desarrolla SSL. Este protocolo se va actualizando hasta su tercera versión.

El IETF estandariza SSL con TLS (v1.0, v1.1, v1.2, v1.3)

2 Seguridad en la capa de transporte

2.1 SSL

Es un protocolo cliente/servidor que proporciona servicios para garantizar prevención contra:

- Ataques de escucha (eveasdropping) -> Confidencialidad
- Ataques de manipulación (tampering) -> Integridad
- Ataques de falsificación (forgery) -> Autenticación

En el caso de SSL (v3.0) se empleaba criptografía híbrida aplicaron RSA, Diffie-Hellman (Fortezza KEA, hasta v3.0).

No garantiza servicio de no-repudio.

La ventaja es que el protocolo de la capa de aplicación solo tiene que basarse en esta capa.

2.1.1 Fases

Se divide en dos fases:

- **Sesión** SSL: negociación de parámetros de seguridad
- **Conexión** SSL: transmisión de datos

2.1.2 Fragmento

Cada fragmento se denomina SSL record que contiene:

- Tipo: protocolo de la subcapa alta
  - SSL Handshake: Negocia cipher suite y opcionalmente un método de compresión
  - SSL Change Cipher Spec Protocol: Permite activar el cipher suite
  - SSL Alert Protocol: Indica posibles problemas e intercambiar mensajes de alerta
  - SSL Application Data Protocol: propio protocol de la capa de aplicación y alimenta al SSL record Protocol
- Versión
- Longitud
- Fragmento

Se divide en las siguientes fases:

- Parámetros de seguridad.
- Enviar certificado (opcional) y posible solicitud del certificado del cliente.
- El cliente lo envía con firma.
- Se establece la suite de cifrado.

2.1.3 Intercambio de claves

La clave de sesión se genera en base a una semilla, un valor aleatorio (nonce) y una función pseudoaleatoria (PRF distinta a TLS):

- Paso 1: Generar números aleatorios (la salt para generar después los parámetros de seguridad comentados anteriormente), establecer el resto de parámetros de seguridad (ej. tipo de algoritmos de intercambio de clave) y enviar toda esta información a la otra parte.
- Paso 2: crear y enviar la semilla "pre-shared master key" mediante ClientKeyExchange.

Diffie Helman efímero permite el Perfect Forward Secrecy (PFS), evitando el riesgo de MiTM.

2.1.4 Handshake

En el Handshake protocol el SSL Record tiene un byte para el tipo, una longitud (3 bytes) y el contenido.

2.1.5 Record

En el SSL Record Protocol se toman los datos de la subcapa alta:

- los fragmenta en bloques manejables,
- los comprime de forma opcional,
- añade el MAC,
- cifra el paquete, y
- añade una cabecera SSL Record

2.2 TLSv1.2 y TLSv1.3

TLSv1.2 se computa la master-key con SHA-256, se quita DES e IDEA y se usa AES con su modos CBC/**GCM** (Galois)/CCM.

TLSv1.3 introduce cambios en rendimiento en un único Round Trip Time (RTT), se limita a CBC y AEAD: GCM y CCM

2.3 DTLS

Es un protocolo encima de UDP, tiene subprotocolos como:

- DTLS handshake protocol
- DTLS change cipher spec protocol
- DTLS alert protocol
- Application protocol

3 Firewalls en redes

Es un sistema (software o hardware) que establece un conjunto de políticas de control. El primero surge a finales de los 80s, debido al malware Morris. Un firewall define:

- Un perímetro de seguridad (por lo general, la misma organización que posee el firewall)
- Una zona de riesgo, sobre la que se realiza la protección

Las zonas desmilitarizadas (De-Militarized Zones) añaden u nivel que permite la conexión con redes externas, pero la conexión a la intranet es prohibitiva.

3.1 Generaciones

Primera generación: filtrado de paquetes (packet filter); se comprobaban parámetros del paquete como la IPs, protocolos, puertos y DNS.

Segunda generación: cortafuegos de estado (stateful inspection); se comprueban además los flags de los paquetes para comprobar el estado de la conexión.

Tercera generación: cortafuegos de aplicación (application filtering); se introduce el concepto de DPI (Deep Packet Inspection), donde se pasa a comprobar el contenido del paquete.

Cuarta generación: cortafuegos de nueva generación (Next-Generation Firewall, NGFW); el objetivo era mejorar servicio de gestión de usuarios, eliminación de aplicaciones no deseadas, protección de sistemas en la nube.

3.2 IpTables

- Permite denegar el tráfico de red entrante y saliente
- Redirigir el tráfico a diferentes puertos
- Filtrar paquetes basados en diferentes criterios
- NAT (Network Address Translation), redirección.

La sintaxis se compone de Input, Output y Forward. La estructura del comando es

iptables -A <chain> -j <target>

- **-A/-D/-I <chain>**: define una cadena de reglas que se agrega tal que:
  - -A : agrega la regla al final de la cadena
  - -D : elimina la regla
  - -I : inserta una nueva regla al principio o en una posición se especifica , y donde <chain>
    - INPUT, entrada
    - OUTPUT, salida
    - FORWARD, forward
- **-s**/--source <ip_origen>
- **-d**/-dest/--destination <ip_destino>
- **-p**/--protocol <protocolo>
- **-j**/--jump <chain>: (jump) especifica el fin de la regla; es decir, qué hacer si un paquete coincide con la regla, como, por ejemplo: ACCEPT y DROP

Para resetear las reglas podemos hacer:

- iptables -F
- iptables -X
- iptables -Z
- iptables -t nat -F

Por otra parte, podemos especificar las políticas por defecto con -P <chain>, siendo chain INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING. Deben ponerse debajo del flush.

El orden importa, dándose más importancia a los primeros.

3.2.1 Prerouting y postrouting

El prerouting de exterior a interior se realiza la función NAT (input/forward).

(Primero FORWARD/OUTPUT y después el POSTROUTING)

El postrouting de interior a exterior (después de NAT) requiere de enmascaramiento.

(Primero el PREROUTING y después FORWARD/INPUT)

3.2.2 TCP

Como estados de TCP podemos indicar el estado con -m state --state y NEW, ESTABLISHED y/o RELATED.

4 SEGURIDAD EN LAS REDES INALÁMBRICAS

Los puntos de ataques son el cliente o estación, el punto de acceso (AP) y el medio de transmisión, mediante robo de identidad, Man-in-the-middle, denegación d eservicio o inyección a la red.

Se clasifican las medidas de acuerdo a:

- La transmisión inalámbrica, posibles de clasificar con técnicas de ocultación o engaño (aleatorización en el routing), cifrado, autenticación de MACs, nonce (DoS)
- El punto de acceso (AP), mecanismo de autenticación.
- Los elementos de interconexión (routers):
    - Cifrar.
    - Deshabilitar broadcast de identificación.
    - Dejar que sólo equipos específicos se conecten por sus MACs.
    - Cambiar el identificador (SID).
    - Cambiar la contraseña (rekeying).

4.1 IEEE 802.11 – WIRED EQUIVALENT PRIVACY (WEP)

Se busca un nivel de seguridad y confidencialidad comparables al de las LAN cableadas. Se basa en una clave de 64 bits compartida entre los dispositivos de la red basándose en el algoritmo de cifrado **RC4**. La vulnerabilidad más notable es el uso de vectores de inicialización pequeños y reutilizables.

4.2 IEEE 802.11I– WI-FI PROTECTED ACCESS (WPA)

Usa el protocolo TKIP inicialmente usando el doble de bits que WEP para el IV, aunque añadiendo/cambiando a **AES** más tarde y protocolo de autenticación 802.1X (EAP, Extensible Authentication Protocol).

Teniendo los servicios de autenticación, control de acceso basado en “puertos” y confidencialidad con integridad de mensaje (HMAC-SHA-1).

Fases

- Descubrimiento con mensajes llamados beacons y probe responses con tal de seleccionar el cipher suite y mecanismo de autenticación
- Autenticación verificando la identidad uno del otro.
- Generación y distribución de claves
- Transferencia segura de datos
- Finalización de conexión

Se define el suplicant (cliente), access point (AP) y authenticator server (AP). Se generan las claves temporales de sesión e PMK (Pairwaise Master Key) y PTK (Pairwise Transient Key).

5 Seguridad en la capa de Internet

IPSec se construye para proporcionar seguridad a nivel de la capade Internet. Nos proporciona:

Autenticación del origen de los mensajes, integridad, confidencialidad e intercambio de calves. Esto es a base de MAC, cifrado y algoritmo de intercambio de claves, **no proporciona servicio no-repudio**, ni protección frente a ataques DoS (aunque protege de algunos ataques).

La comunicación en IPSec utiliza los siguientes subprotocolos:

- ESP (Encapsulating Security Payload), confidencialidad, integridad y autenticación.
- AH (Authentication Header), integridad y autenticación.
- IKE (Internet Key Exchange), generación y distribución de claves.

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

El DOI (Dominio de Interpretación) contiene valores necesarios para relacionar documentos.

5.1 Modos

IPSec se divide en dos modos:

- Transporte, punto a punto entre dos hosts, protección a payload.
  - ESP, no la cabecera IP
  - AH, algunas porciones de la cabecera
- Túnel, comunicación entre gateways y routers, protección a todo el paquete IP
  - ESP, cifra el paquete interno
  - Todo el paquete original y algunas partes de la nueva cabecera,

5.2 Asociación de seguridad

Protege en un sentido y sirve par configurar los parámetros de seguridad, autenticación, algoritmo de cifrados, secuencias de números y SPO, índice único de cada asociación de seguridad definida (**SPI**)…

La base de datos de asociaciones de seguridad (SAD), guarda SPI, AH Information ESP Information y Lifetime of the SA, pudiendo incluir el tipo de modo.

Para especificar cómo va a viajar el tráfico entre dos puntos se necesita una política de seguridad SP, que se almacena en una base de datos (SPD), incluye así el modo de protección.

5.3 IKE

Cuando no existe una asociación de seguridad, IKE se encarga de la autenticación de ambas partes y establece la clave secreta; usa protocolos como Oakley, ISAKMP.

La autenticación puede estar basada en claves compartidas, RSA o certificados x.509 con dos posibles modos agresivo (rápido, pero entidad del cliente en claro) y principal (seguro, pero más lento). El nuevo SA ISAKMP se emplea para negociar y establecer los SA de IPSex

Test

1 ¿Cuál es el objetivo principal de la firma dual?

a. **Enlazar dos mensajes que han de ir a receptores diferentes**
b. Involucrar a una tercera parte confiable en el protocolo
c. Ocultar el mensaje de pago y el mensaje del pedido
d. Encadenar varios hashes de la siguiente forma: H(H(OI)||H(PI))

2 El handshake de SSL consta de hasta ...

a. Algoritmos de cifrados propietarios
b. Un total de 6 subfases
c. Cabecera y estado
d. **Un total de cuatro fases**

3 Un robo de información y un robo de configuración de red, se puede considerar ...

a. **una amenaza a la confidencialidad**
b. ataques completos
c. un ataque a la integridad de los datos
d. un ataque a la integridad de la persona

4 Si hablamos del protocolo SSL nos referimos a....

a. **Una subcapa entre la de aplicación y la de transporte**
b. Una librería para implementar operaciones criptográficas
c. Un criptosistema asimétrico
d. Un sistema de cifrado simétrico

5 Podemos afirmar que el protocolo SSL/TLS tiene ...

a. **Varios subprotocolos**
b. Varios subprotocolos para la subcapa de aplicación
c. Dos estados con varios subprotocolos

d. Varios estados

6 En la sesión de SSL/TLS ...

a. Se transmiten los datos
b. Se comparten los secretos
c. Todas las restantes son incorrectas
d. Se negocian los parámetros de seguridad

7 Tanto en SSL como en TSL se hace uso de Diffie Helman Efímero para ...

a. Inicializar el IV
b. Evitar un ataque de Man in the Middle
c. Computar los hash MD5
d. Todas las anteriores son equivocadas

8 SET asegura:

a. Confidencialidad, autenticidad y no-repudio
b. Confidencialidad, autenticidad, privacidad, integridad y no-repudio
c. Confidencialidad, autenticidad, privacidad, integridad y repudio
d. Confidencialidad, autenticidad, integridad y repudio

9 Elige la respuesta que NO este relacionada con OpenID Connect

a. OpenID Connect proporciona autenticación
b. OpenID Connect se basa en OAuth 2
c. OpenID Connect proporciona control de acceso (autorización) basada en tokens
d. OpenID Connect es el sucesor de OpenID

10 RESPUESTA MÚLTIPLE: Elige los códigos de acceso (tokens) que OAuth 2 proporciona:

a. Código de Refresco
b. Código de Control
c. Token OAuth2
d. Código de Acceso

11 ¿Qué es OWASP?

a. Organización sin ánimo de lucro dedicada a combatir el cibercrimen organizado
b. Organización sin ánimo de lucro dedicada a registrar vulnerabilidades de seguridad conocidas en software existente.
c. **Organización sin ánimo de lucro dedicada a determinar las causas que hacen que el software sea inseguro, y proporcionar contramedidas**
d. Organización sin ánimo de lucro dedicada a estandarizar servicios de seguridad

12 RESPUESTA MÚLTIPLE - ¿CÓMO EVITAR UN ATAQUE DE SQL INJECTION?

a. **Usando consultas parametrizadas (Parameterized Queries)**
b. Utilizando Node.JS en vez de otros lenguajes vulnerables como PHP
c. Haciendo un hash a todos los parámetros, sin excepción
d. **Minimizando los privilegios del usuario que acceda a la BBDD**

13 ¿EN QUÉ CONSISTE EL ATAQUE XSS?

a. En realizar peticiones web no deseadas en nombre del usuario que tiene la sesión iniciada
b. En inyectar comandos de Linux
c. En modificar la lógica de acceso a la página web
d. **En insertar datos no validados (p.ej. scripts) en páginas web dinámicas de forma (in)directa**

14 SI EN TOR LA RUTA A TOMAR ES: R2 -> R3 -> R15 -> R17, ENTONCES LA COMUNICACIÓN SE DEBERÍA PROTEGER DE LA SIGUIENTE FORMA:

a. KpubR17(KpubR15(KpubR3(KpubR2(M))))
b. **KpubR2(KpubR3(KpubR15(KpubR17(M))))**
c. KpubR2(KpubR3(KpubR17(KpubR15(M))))
d. KpubR17(KpubR3(KpubR15(KpubR2(M))))

15 ¿QUÉ ES EL "ANONIMATO NO RASTREABLE"?

a. El que únicamente se basa de técnicas para ocultar la identidad de un usuario a través de pseudónimos
b. El que garantiza que la identidad de los usuarios no se puede revelar, y que el conjunto de las operaciones realizadas por un usuario anónimo no se puedan vincular
c. **El que implementa técnicas mucho más estrictas desde el punto de vista a la privacidad del usuario para evitar su rastreo**
d. El que implementa pseudónimos donde la identidad del usuario original se "comparte" entre dos o más partes implicadas

16 ¿CUÁL ES LA CARACTERÍSTICA PRINCIPAL DE LA FIRMA EN ANILLO?

a. El firmante firma mensajes para otros usuarios, pero desconoce el contenido de los mensajes que firma
b. Cualquier miembro del grupo firma mensajes de forma parcialmente anónima en nombre del grupo
c. **Cualquier miembro del grupo firma mensajes de forma completamente anónima en nombre del grupo**

d. La firma la producen conjuntamente un mínimo de t usuarios, en nombre del grupo de n usuarios (t < n) del que forman parte

17 SELECCIONA EJEMPLOS DE LAS PROPIEDADES O CONDICIONES INICIALES QUE DEBE SATISFACER UN ESQUEMA DE FIRMA DE GRUPO

a. Un grupo k de miembros del grupo pueden conocer qué miembro del grupo ha firmado el mensaje
b. Los miembros no pueden evitar la apertura de la firma por parte del administrador, ni firmar por otro
c. El miembro firmante no puede conocer el contenido del mensaje
d. Todas las anteriores

18 ¿CÓMO ES UNA SOLUCIÓN DE PRIVACIDAD BASADA EN UN PROXY?

a. Un servidor crea un paquete cifrado en capas, que se irán "pelando" a medida que atraviese el camino
b. Varios servidores se agrupan, y todos enrutan de manera aleatoria los paquetes recibidos de sus compañeros
c. Un servidor hace de intermediario en la comunicación, aceptando conexiones de los clientes y reenviándolas
d. Un servidor almacena las comunicaciones de varios clientes, y las envía mezcladas

19 EN UNA CONEXIÓN TOR, ¿DÓNDE SE ENCUENTRA LA CONEXIÓN NO CIFRADA?

a. Entre el origen y el segundo nodo del canal de comunicaciones
b. Entre el penúltimo nodo del canal de comunicaciones y el destino
c. Todas las conexiones se encuentran cifradas
d. Todas las comunicaciones se encuentran "en abierto"

20 "LA INCAPACIDAD DE UN ATACANTE PARA RELACIONAR DOS MENSAJES O ENTIDADES OBSERVADAS" CORRESPONDE A:

a. Anonimato
b. no-observación
c. anonimato no rastreable
d. no-vinculación

21 LA FIRMA CIEGA SE BASA EN:

a. M' = M.r^d mod n
b. M' = M.r^(r-1) mod n
c. M' = M.r^e mod n
d. M' = M.r^(de) mod n

22 En SSL/TLS podemos decir que ...

a. DHE no es compatible con RSA
b. Se puede usar o DHE o RSA
c. DHE es compatible con RSA
d. Todas las anteriores son incorrectas

23 Relación entre TLS y SSL:

a. SSL supone una mejora significativa a TLS
b. TLS es una estandarización de SSL
c. Todas las anteriores son incorrectas
d. SSL es una estandarización de TLS

24 El ámbito de la funcionalidad de SSL/TLS es ...

a. Todas las anteriores son incorrectas
b. Doble, negociar los parámetros de seguridad y establecer una conexión segura
c. Transmitir datos seguros a nivel de aplicación
d. Establecer una conexión segura

25 Podemos afirmar que en SSL/TLS se computan ...

a. Una clave de sesión, una clave para el MAC y un vector de inicialización para computar el modo de operación
b. Una clave de sesión y una clave para el MAC
c. Todas las otras respuestas son incorrectas
d. Un IV y de ahí se extraen una clave de sesión y una clave para el MAC

26 Considerando el tema de SSL/TLS, podemos afirmar ...

a. Una desventaja del protocolo SSL/TLS es que es independiente de la capa de aplicación
b. Cualquier protocolo de aplicación basado en TCP se puede beneficiar de SSL/TLS
c. SSL/TLS no están limitados con los protocolos de capa de aplicación con los que operar
d. Todas las otras respuestas son incorrectas

27 SSL Record Protocol ...

a. Se usa para comunicar al otro punto de la comunicación las alertas relacionadas con SSL
b. Toma los datos de la subcapa alta, los fragmenta en bloques manejables, los comprime de forma opcional, añade el MAC, cifra el paquete y añade una cabecera SSL record
c. Es un protocolo muy simple que consta de un solo mensaje de un sólo byte con valor 1 que permite activar el cipher suite
d. Ninguna de las anteriores es correcta

Bibliografía

Tema 5 – Seguridad en redes