“Protocolos Seguros”

Trabajo Preparatorio N°13

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el presente documento se presenta el fundamento teórico acerca de Protocolo Seguro, con el fin de reforzar conocimientos a protocolos de seguridad en las diferentes capas de pila TC/IP mediante la recolección de capturas de trafico de los diversos protocolos seguros de la capa2, capa 3 y capa 4. con los diferentes protocolos como WPA que sirve para proteger redes WIFI, IPSec que ayuda asegurar comunicaciones IP y finalmente SSL-TLS que mantiene segura una conexión a Internet.**

***Index Terms*—Protocolo, WIFI, WPA, IPSec, SSL-TLS, TCP-IP.**

I. Introducción

Los protocolos seguros son protocolos que usan técnicas criptográficas y cuyo objetivo es conseguir que entidades colaboren con su información preservando su privacidad y confidencialidad [1].

Los protocolos de seguridad que nombran el protocolo criptográfico o de cifrado ayudan a proteger los datos confidenciales, los datos financieros y la transferencia de archivos mediante el método criptográfico [1]. Los protocolos de seguridad pueden aplicar computación segura de múltiples partes, proceso de intercambio secreto, autenticación de entidad, método de no repudio, método de encriptación.

II. Objetivo

- Reforzar los conocimientos del alumno relativos a protocolos de seguridad en las diferentes capas de la pila TCP/IP.

III. Cuestionario

A. Consultar el funcionamiento y características principales de WPA. (máximo 1 carilla).

WPA es uno de los tipos de protocolos de seguridad para acceder a Wi-Fi y fue desarrollado para proteger redes inalámbricas de computadoras. Admite dos modos de autenticación: personal y empresarial. Wi-Fi Alliance desarrolló WPA como un esquema de seguridad en respuesta a las deficiencias de WEP (Wired Equivalent Privacy) [2].

Los siguientes son los aspectos más importantes de WPA:

- Administración de claves autenticadas: ya sea mediante la autenticación 802.1x o una clave previamente compartida, el usuario se autentica antes de la autenticación de las claves utilizadas.
- Administración de claves de difusión y unidifusión: las claves derivadas después de la autenticación del usuario se autentican mediante un proceso de reconocimiento entre el punto de acceso y el cliente.
- TKIP (codificación por paquete) y MIC
- Expansión del espacio IV: El espacio IV se expande de 24 bits, como en 802.11 WEP, a 48 bits en WPA [3].

Beneficios de WPA

- WPA proporciona un apoyo encomiable para servidores RADIUS o servidores de autenticación.
- El soporte de autenticación incorporado está disponible [3].
- WPA usa algoritmos mucho mejores y más fuertes que WEP, su predecesor.
- WPA3 utiliza los últimos métodos de seguridad y no permite protocolos heredados obsoletos.
- WPA3 también permite a los usuarios elegir sus contraseñas para que sea fácil de recordar [2].
- El tráfico de datos permanece protegido incluso si la contraseña se ve comprometida después de la transmisión de datos [2].

Limitaciones de WPA

- Carece de seguridad hacia adelante [3].
- El mayor problema con WPA es su incompatibilidad con el hardware heredado y otros sistemas operativos.
- Tiene una sobrecarga de rendimiento mucho mayor.
- WPA aumenta el tamaño del paquete de datos y conduce a una transmisión más larga [4].

B. Consultar el funcionamiento, cabecera, y características principales de IPSEC.(máximo 2 carillas).

IPSec (Internet Protocol Security) es una colección de extensiones de protocolo para el Protocolo de Internet (IP) [5]. Las extensiones permiten el cifrado y la información transmitida con IP y garantizan una comunicación segura en redes IP como Internet. Con Internet Protocol Security es

posible cifrar datos y autenticar a los socios de comunicación. Puede proteger el intercambio de información en redes potencialmente inseguras como Internet [6].

IPSec es el método más seguro disponible comercialmente para conectar sitios de red. IPSec fue diseñado para proporcionar las siguientes características de seguridad al transferir paquetes a través de redes:

- Autenticación: verifica que el paquete recibido sea en realidad del remitente reclamado.
- Integridad: garantiza que el contenido del paquete no haya cambiado durante el transporte.
- Confidencialidad: oculta el contenido del mensaje mediante cifrado [7].
- Anti-repetición: Evita que los usuarios malintencionados envíen repetidamente los paquetes capturados. Esto significa que el receptor rechaza paquetes antiguos o repetidos.

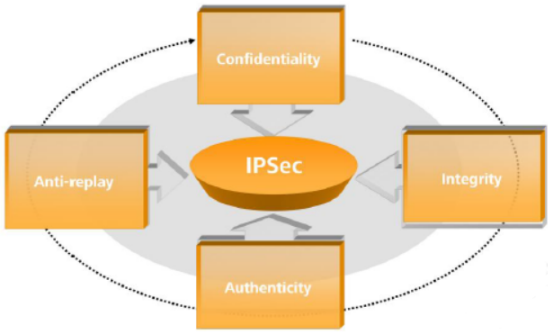

Fig. 1. Características de IPSec

La seguridad del protocolo de Internet (IPSec) tiene dos modos:

1) **Modo de transporte:** El modo de transporte crea una conexión directa punto a punto entre dos puntos finales, para hacer esto, usa un encabezado IPsec adicional entre el encabezado IP y los datos transportados [8].
2) **Modo túnel:** En el modo de túnel, dos redes conectadas a través de un túnel seguro entre dos puertas de enlace o enrutadores. Además, los dispositivos finales conectados a través de las dos redes no tienen que ser compatibles con la seguridad del protocolo de Internet [8].

IPSec combina dos mecanismos fundamentales que se articulan para garantizar la completa privacidad de la información enviada. Estos mecanismos son la cabecera de autentificación (AH) y la capa de seguridad encapsulada (ESP) [7].

- **Cabecera de autentificación (AH):** La función de la cabecera de autentificación de IPSec, más conocida simplemente como AH, consiste en la incorporación de una firma digital en cada paquete de datos enviado. La AH permite verificar que solo el destinatario de los datos pueda recibirlos, y a su vez impide que los datos sean modificados antes de llegar a su destino, evitando, por ejemplo, los ataques de intermediario [6].
- **Capa de seguridad encapsulada (ESP):** Complementaria a la AH, la capa de seguridad encapsulada (ESP) tiene la función de asegurar la encriptación de la información que se encuentra dentro del paquete, de forma que impide que los datos enviados sean accesibles por parte de terceros que puedan interceptar una transmisión. Utiliza tres partes fundamentales para operar: un encabezado ESP, un tráiler y un bloque de verificación [6].

Gestión de claves

IPSec utiliza el protocolo Internet Key Exchange (IKE) para facilitar y automatizar la configuración de SA y el intercambio de claves entre las partes que transfieren datos. El uso de claves asegura que solo el remitente y el receptor de un mensaje puedan acceder a él. IPSec requiere que las claves se vuelvan a crear o se actualicen con frecuencia para que las partes puedan comunicarse de forma segura entre sí. IKE gestiona el proceso de actualización de claves; sin embargo, un usuario puede controlar la fuerza de la clave y la frecuencia de actualización. Actualizar las claves de forma regular garantiza la confidencialidad de los datos entre el remitente y el receptor [8].

IPSec con otros protocolos

Cuando opera en el contexto de una VPN, IPSec suele utilizarse en combinación con otros protocolos para garantizar la seguridad de los datos y la velocidad de la conexión. Los más comunes son IKEv2 y L2TP.

- **IPSec con IKEv2 (IKEv2/IPSec):** IKEv2 (Internet Key Exchange version 2) es un protocolo desarrollado por Microsoft y Cisco. Se trata de un protocolo de túnel que cuenta con la principal ventaja de ser particularmente flexible a los cambios de la red, además de ser compatible con diversos sistemas operativos. Usar IPSec con IKEv2 VPN garantiza una conexión robusta con una gran velocidad y estabilidad [9].
- **IPSec con L2TP (L2TP/IPSec):** El protocolo L2TP (Layer 2 Tunnel Protocol) es un protocolo de túnel que carece de encriptación por sí mismo, de ahí que sea necesario utilizarlo en combinación con un protocolo que sí la tenga, como IPSec. La principal ventaja de L2TP es su velocidad, con lo que muchas VPNs eligen la combinación L2TP/IPSec para garantizarles a sus usuarios una conexión rápida y segura [9].

Ventajas

- IPSec es prácticamente indetectable, de ahí que tantas VPN lo elijan como su protocolo principal [8].
- IPSec opera en la capa de red en lugar de hacerlo en la capa de aplicación, lo que significa que puede gestionarse en su totalidad desde el sistema operativo, sin necesidad de hacerlo de forma individual desde cada programa [7].

Desventajas

- IPSec envuelve cada paquete con una gran cantidad de información, por lo que puede ralentizar la transmisión de paquetes de datos pequeños.
- IPSec es un protocolo bastante más complicado que otros protocolos similares, lo que dificulta su mantenimiento [9].

C. Consular que es y para qué sirve el protocolo Internet Key Exchange. (máximo 1 carilla).

Este protocolo IKE (Internet Key Exchange) se utiliza para generar y administrar las claves necesarias para establecer las conexiones AH (Cabecera de autenticación) y ESP (Carga de Seguridad Encapsulada). Los dos o más participantes de la conexión IPsec deberán acordar de alguna manera, los tipos de cifrados y los algoritmos de autenticación para poder establecer la conexión de una forma segura. Esta configuración se podrá hacer de forma manual a ambos extremos del canal, o a través de un protocolo (el protocolo IKE) para que se encargue de la negociación automática de los participantes (SA = Asociación de Seguridad). [5]

El protocolo IKE no sólo se encarga de la gestión y administración de las claves, sino también del establecimiento de la conexión entre los participantes correspondientes. IKE no sólo está en IPsec, sino que puede ser usado en los distintos algoritmos de enrutamiento como OSPF o RIP.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad se lleva a cabo en dos fases: [10]

Primera fase: La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado. Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

- El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente utilizando certificados digitales X509v3.

Segunda fase: el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado. Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado.

D. Consultar el funcionamiento y características principales de SSL-TLS. (máximo 1 carilla).

El SSL/TLS emplea cifrados simétricos y asimétricos para proteger la confidencialidad e integridad de los datos en tránsito. El cifrado asimétrico se utiliza para establecer una sesión segura entre cliente y servidor, y el simétrico para intercambiar datos dentro de la sesión segura. Un sitio web debe tener un certificado SSL/TLS para que su servidor web/nombre de dominio utilice el cifrado SSL/TLS. Una vez instalado, el certificado permite al cliente y al servidor negociar de forma segura el nivel de cifrado en los siguientes pasos: [11]

1) El cliente se pone en contacto con el servidor mediante una URL segura (HTTPS...).

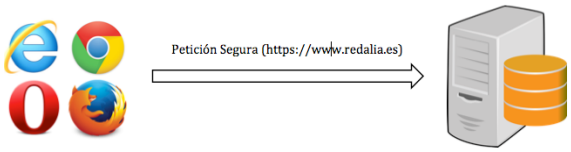

Fig. 2. Contacto con el servidor

2) El servidor envía al cliente su certificado y clave pública.

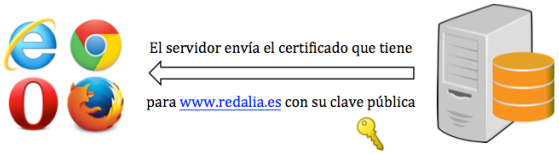

Fig. 3. Envió de certificado y clave publica

3) El cliente verifica esto con una autoridad de certificación raíz de confianza para comprobar que el certificado es legítimo.
4) El cliente y el servidor negocian el tipo de cifrado más potente que ambos pueden resistir.
5) El cliente cifra una clave de sesión (secreta) con la clave pública del servidor y se la devuelve al servidor.

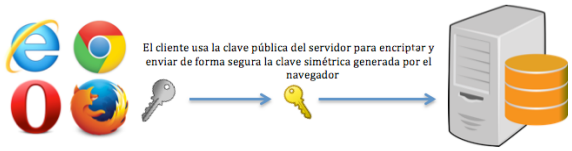

Fig. 4. Cifrado de clave secreta

6) El servidor descifra la comunicación del cliente con su clave privada y se establece la sesión.
7) Ahora se usa la clave de sesión (cifrado simétrico) para cifrar y descifrar los datos transmitidos entre el cliente y el servidor.

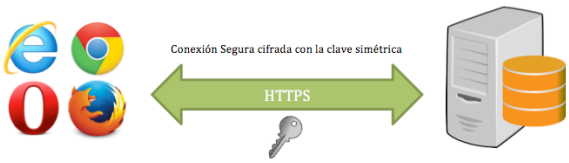

Fig. 5. Comunicación segura

Tanto el cliente como el servidor usan ahora HTTPS (SSL/TLS + HTTP) para sus comunicaciones. Los navegadores validan esto con un icono de candado en la barra de direcciones del navegador. El HTTPS funciona sobre el puerto 443.

Con el protocolo SSL/TLS los Certificados de Seguridad poseen cuatro características para proteger la información: cifrado, integridad, autenticación y ausencia de rechazo. [12]

- El cifrado transforma los datos para que sean legibles, únicamente, por las partes interesadas.
- La integridad implica que no se pueden interceptar ni alterar mientras viajan en las redes.
- La autenticación es un proceso de validación y verificación para comprobar la existencia legal de la empresa y que es dueña del sitio web.
- La ausencia de rechazo reúne las características anteriores para dar certeza de quiénes y cómo realizaron las transacciones en línea.

REFERENCES

[1] "Different Security Protocols that Secures your Data Integrity", ClickSSL Blog - Information about SSL Certificates & Infosec. https://www.clickssl.net/blog/different-security-protocols-that-secures-your-data-integrity (accedido sep. 08, 2021).

[2] "What's WPA and Why Do You Need It?", Lifewire. https://www.lifewire.com/definition-of-wifi-protected-access-816576 (accedido sep. 08, 2021).

[3] "WPA Full Form — What Is The Full Form of WPA?", BYJUS. https://byjus.com/gate/wpa-full-form/ (accedido sep. 08, 2021).

[4] S. Richardson,"WPA Characteristics - Cisco Autoqos", Cisco Certified Expert, sep. 19, 2012. https://www.ccexpert.us/cisco-autoqos/wpa-characteristics.html (accedido sep. 08, 2021).

[5] "Mejora la seguridad de tu VPN con el protocolo IPsec". (2021). https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/ (accedido sep. 08, 2021).

[6] "What is IPsec? - Definition, Features, Modes, and More", Computer Tech Reviews, ene. 20, 2020. https://www.computertechreviews.com/definition/ipsec/ (accedido sep. 08, 2021).

[7] "Que es y caracteristicas de una IPSec VPN", Comunidad Huawei Enterprise. https://forum.huawei.com/enterprise/es/que-es-y-caracteristicas-de-una-ipsec-vpn/thread/537837-100233 (accedido sep. 08, 2021).

[8] Cisco, "Overview of the IPsec Features", p. 10.

[9] "IPSec. ¿Qué es y cómo funciona? — NordVPN", mar. 07, 2021. https://nordvpn.com/es/blog/protocolo-ipsec/ (accedido sep. 08, 2021).

[10] "El protocolo IKE (INTERNET Key Exchange)". https://1library.co/article/protocolo-ike-internet-key-exchange-las-especificaciones-ipsec.y86l175q (accedido sep. 08, 2021).

[11] "Cifrado SSL/TLS" https://www.f5.com/es_es/services/resources/glossary/ssl-tls-encryption (accedido sep. 08, 2021).

[12] "10 Ventajas de tener un certificado SSL/TLS". https://www.certsuperior.com/10-ventajas-de-tener-un-certificado-ssl-tls/ (accedido sep. 08, 2021).