“Protocolos Seguros”

Informe 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 siguiente documento se presentará el análisis acerca de protocolos seguros analizados en diferentes archivos que fueron analizados en base al software Wireshark.**

***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. *Explique los resultados obtenidos durante la práctica.*

A continuación se presentan los resultados obtenidos durante la sesión de laboratorio.

- Análisis del archivo “Captura_WIFI.pcap”
  WPA2 (Wifi Protected Access 2) puede utilizar el cifrado de cifrado TKIP (Protocolo de integridad de clave temporal) o el cifrado de cifrado AES (Estándar de cifrado avanzado) [2]. Ahora, PSK (clave precompartida) es un método de autenticación de cliente que genera claves de cifrado únicas basadas en la frase de contraseña alfanumérica (hasta 133 caractéres) y el nombre de la red (SSID), en base a lo que se obtienen los parámetros 1 y 2 presentes en la tabla I.
  Generalmente, se recomienda utilizar AES cuando se utiliza WPA2-PSK, es así como en este se utiliza dicho método en este ejemplo al analizar el parámetro 5. Asimismo, se conoce que existen 2 clientes debido a que se puede obtener las direcciones MAC de dichos usuarios. Finalmente, es importante mencionar que se pueden obtener las credenciales de acceso mediante el uso de ataques de fuerza bruta con lo que se puede leer información sensible que es transmitida en la red.

Tabla I.
Resultados obtenidos de WPA

Parámetro	Valor
1. Nombre de la red	Coherer
2. BSSID	Cisco-Li_82:b2:55 (00:0C:41:82:B2:55)
3. Canal utilizado	1
4. Clientes conectados	2---> 00:0D:93:82:36:3A & 00:0D:1D:06:E0:F2
5. Tipo de Seguridad	WPA2 & PSK
6. Credenciales de Acceso	Induction
7. IP y recurso accedido en paquete 74	66.230.200.100 /wiki/LandsharkHTTP/1.1

WPA2 mejoró la versión anterior con dos nuevos protocolos:

- 4-way handshake – negociación de 4 mensajes
- Group key handshake – negociación de clave de grupo

El handshake de 4 caminos está diseñado de modo que el AP, o authenticator, y el cliente inalámbrico, o supplicant, puedan independientemente proveer al otro la clave que conocen para el PSK/PMK, sin comprometerla, por supuesto. En vez de enviar la clave al otro nodo, el AP y el cliente cifran un mensaje para el otro, que solo puede ser descifrado con la PMK que han compartido, y si el mensaje puede ser descifrado satisfactoriamente, esto provee información de la PMK. La PMK es generada luego de toda la sesión, y debería ser expuesta lo menos posible al medio. No obstante, las claves para cifrar el tráfico sí deben ser enviadas. El handshake de 4-way es utilizado para establecer otra clave, llamada PTK (pairwise Transient Key) [2].

Funcionamiento:

El intercambio real del 4-way handshake son los siguientes, y todos viajan en forma de tramas EAPOL-key:

1) El AP envía un valor nonce al cliente. Este valor se llama Anonce. El cliente genera su propio nonce, llamado Cnonce, y ahora tiene todos los atributos para construir la PTK [2].
2) El cliente envía su propio Cnonce al AP junto con un código de integridad de mensaje, o MIC, que permite verificar la autenticidad. Es, en realidad, un HMAC (Hash message authentication code) o, específicamente aquí, MAIC (message authentication and integrity code).
3) El AP construye y envía al cliente la GTK o clave de grupo, y una secuencia de números acompañada de con otro MIC. Esta secuencia de números será utilizada en la siguiente trama broadcast o multicast, de modo que al recibirla, el cliente puede ejecutar una detección básica de replay [2].
4) El cliente envía finalmente una confirmación, o acknowledge (ACK) al AP.

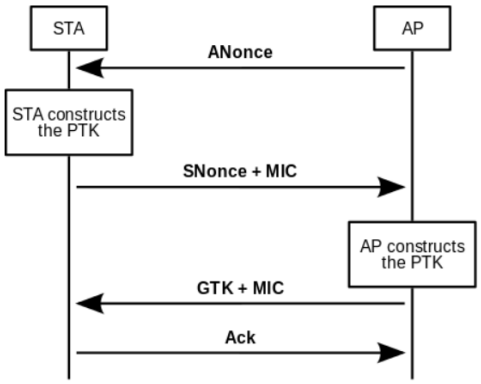
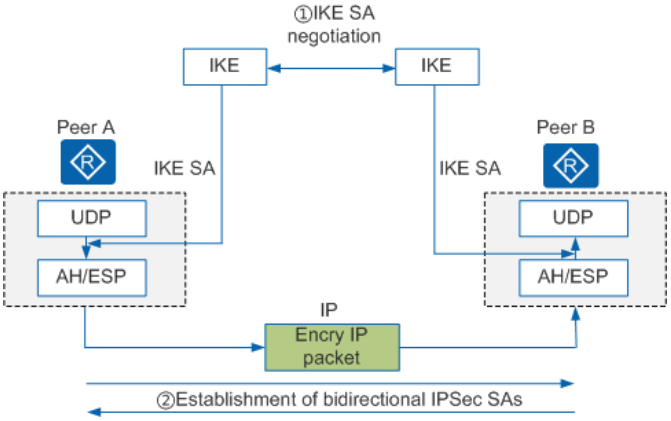


Fig. 1. Handshake de 4 vías

- Análisis del archivo "Captura_IPSEC.pcap"
El protocolo IKE trabaja en el puerto 500 su modo de funcionamiento es agresivo lo que permite especificar atributos de túnel "radius" para seguridad IP (IPsec) e iniciar una negociación de modo agresivo de intercambio de claves de Internet (IKE) con los atributos del túnel.

Modos de Operación.

Hay dos modos de operación para el primer paso: el modo principal, que se utiliza para proteger la identidad de los pares, y el modo agresivo, que se usa cuando la seguridad de la identidad de los pares no es un tema importante. Durante el segundo paso, los pares utilizan el canal de comunicación seguro para establecer negociaciones de seguridad en nombre de otros servicios como IPSec. Estos procedimientos de negociación dan lugar a dos canales unidireccionales de los cuales uno es de entrada y el otro de salida. El modo de operación para el segundo paso es el modo rápido [4].
A continuación se presenta el diagrama de IKE.



Para este caso, al trabajar con ESP se puede proporcionar integridad a los datos, cifrado, autenticación y anti-reproducción; con lo que el nivel de seguridad aumenta.

Tabla II.
Resultados obtenidos de IPSEC

Parámetro	Valor
1. Puerto usado por el protocolo IKE	500
2. Modo de funcionamiento empleado en la fase 1 de IKE	Aggressive
3. Algoritmo de cifrado propuesto en la fase 1 de IKE por quien inicia la comunicación	AES-CBC
4. Algoritmo de Hash propuesto en la fase 1 de IKE por quien inicia la comunicación	SHA
5. Método de autenticación propuesto en la fase 1 de IKE por quien inicia la comunicación	PSK (Pre-shared key)
6. Longitud de la clave propuesta en la fase 1 de IKE por quien inicia la comunicación	256 bits
7. Valor del hash que ha sido calculado haciendo uso de la clave precompartida por ambos extremos (En hexadecimal)	5128e70bee1b057b936efd52124f66 fb4cc537ac
8. Protocolo de IPSEC que ha sido acordado por los extremos en la fase 2 de IKE para ser usado	ESP (Encap Security Payload)
9. ESP SPI de quien inicia la comunicación	0x80f627c9 (2163615689)
10. ESP SPI del destino de la comunicación	0x9a1fd602 (2585777666)

- Análisis del archivo "Captura_SSL-TLS.pcap"
SSL (Secure Sockets Layer) y su sucesor TLS (Transport Layer Security), son protocolos para establecer enlaces autenticados y encriptados entre computadoras en red, es así como en la tabla III se observa que la versión con la que se trabaja es TLS 1.0 debido a que los datos obtenidos son del año 2007 aproximadamente, en dicho tiempo SSL ya había sido reemplazado por TLS. SSL/TLS funciona mediante la vinculación de las identidades de entidades como sitios web y empresas a la criptografía pares de llaves a través de documentos digitales conocidos como Certificados X.509. Cada par de claves consta de un llave privada y una llave pública. La clave privada se mantiene segura y la clave pública se puede distribuir ampliamente a través de un certificado.

Tabla III.
Resultados obtenidos de SSL

Acción	Regla
1. Dirección IP del cliente	10.0.0.1
2. Dirección IP del servidor	10.0.0.2
3. Versión de SSL-TLS usada	TLS 1.0
4. Puerto usado por el cliente en la comunicación	1162
5. Puerto usado por el servidor en la comunicación	443
6. Opción de cifrado seleccionada por el servidor	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
7. Fecha de caducidad del certificado del servidor (dd/mm/yyyy)	24/10/2007
8. Longitud de la clave pública usada por el servidor en Diffie-Hellman	128 bits
9. Longitud de la clave pública usada por el cliente en Diffie-Hellman	128 bits
10. Longitud del primer mensaje TLS, con datos de la capa de aplicación, enviado por el cliente	544
11. Longitud del primer mensaje TLS, con datos de la capa de aplicación, enviado por el servidor	848

Los certificados SSL/TLS funcionan al vincular digitalmente una clave criptográfica a la información de identificación de una empresa. Esto permite cifrar las transferencias de datos de tal manera que no puedan ser descifrados por terceros.

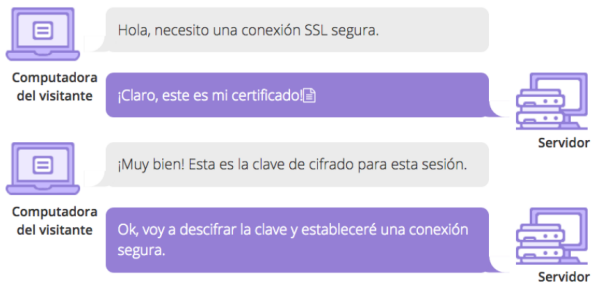


Fig. 2. Envío de mensajes [5]

El protocolo TLS funciona al tener tanto una clave privada como una pública, así como claves de sesión para cada sesión segura única. Cuando un visitante escribe una dirección con seguridad HTTPS en su navegador web o navega a través de una página segura, el navegador y el servidor web se conectan [6].

Durante la conexión inicial, las claves pública y privada se utilizarán para crear una clave de sesión [5], que luego se utilizará para cifrar y descifrar los datos que se transfieren. Esta clave de sesión seguirá siendo válida por un tiempo limitado y solo se utilizará para esa sesión en particular [6].

B. Conclusiones

- WPA-PSK es un sistema de cifrado que permite autenticar a los usuarios en redes de área local inalámbricas es así como la transmisión de datos se cifra y se controla mediante la contraseña generada por el usuario final.
- SSL es una herramienta muy importante que posee una conexión a internet segura para proteger cualquier información que sea confidencial que permite realizar transacciones exitosas online por eso es muy conocida y utilizado en negocios.
- Las versiones 1.0 y 1.1 de TLS se ven afectadas por una gran cantidad de vulnerabilidades de protocolo e implementación que han sido publicadas por investigadores de seguridad en las últimas dos décadas, por lo cual su uso es cada vez menos frecuente.

C. Recomendaciones

- Revisar a detalle cada uno de las pestañas presentes en los datos capturados con el fin de poder analizar y llegar a conclusiones más concretas acerca de cada uno de los valores obtenidos.
- Verificar cada uno de los paquetes que se tiene en las capturas de tráfico para identificar cada uno de los parámetros que ya se sabe debido a al definición.
- Las claves de autenticación de WPA2 es vulnerable a password cracking por fuerza bruta, por lo que se recomienda siempre el uso de claves de alrededor de 20 caractéres.

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. 14, 2021).

[2] WPA2-PSK, “Wifi Protected Access 2”, WPA2-PSK. https://www.wpa2-psk.com/ (accedido sep. 16, 2021).

[3] “What is a Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)? - Definition from Techopedia”, Techopedia.com. http://www.techopedia.com/definition/22921/wi-fi-protected-access-pre-shared-key-wpa-psk (accedido sep. 16, 2021).

[4] ”Intercambio de claves de internet(ike)”. Techinfo. https://techinfo.wiki/intercambio-de-claves-de-internet-ike/. (accedido sep. 17, 2021).

[5] “¿Qué Es SSL? - Guía Completa sobre Seguridad Web”, Tutoriales Hostinger, nov. 19, 2018. https://www.hostinger.es/tutoriales/ssl-tls-https (accedido sep. 17, 2021).

[6] “¿Qué es SSL? - SSL .com”, SSL.com. https://www.ssl.com/es/preguntas-frecuentes/faq-que-es-ssl/ (accedido sep. 17, 2021).