UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Ingeniería e Investigaciones Tecnológicas

Seguridad y Calidad en Aplicaciones Web

Unidad N° 3: Anexo Protocolos de Comunicación Segura

Fuente: "Criptografía y Seguridad en Computadoras", Manuel José Lucena López. Capítulo 16, Protocolos de Comunicación Segura

Capítulo 16

Protocolos de Comunicación Segura

16.1. Introducción

Quizás la aplicación más antigua de la Criptografía sea precisamente la de establecer canales de comunicaciones seguros entre dos puntos. Desde un soldado galopando a través de territorio enemigo hasta un haz láser, pasando por un hilo telegráfico, el ser humano ha empleado infinidad de medios para poder enviar sus mensajes, cada uno de ellos con sus propias peculiaridades. Pero si hay una característica que podemos considerar común a todos los canales de comunicaciones, es la ausencia de control que sobre el mismo poseen ambos interlocutores. En el caso del jinete, sería muy interesante poder crear un pasillo de territorio *amigo* a lo largo de todo su trayecto, pero en ese caso su propia tarea carecería prácticamente de sentido. En general, hemos de considerar que nuestros mensajes son depositados en un medio ajeno a nosotros —y usualmente hostil—, y que los medios que apliquemos para su protección deben ser válidos en los casos más desfavorables.

Un mensaje liberado en un medio hostil se enfrenta principalmente a dos peligros:

- Acceso por agentes no autorizados. En un medio sobre el que no podemos ejercer ningún control, esta posibilidad debe tomarse muy en serio. Tanto que en lugar de suponer que el *enemigo* puede acceder al mensaje, hemos de dar por hecho que va a hacerlo. Por lo tanto, nuestros sistemas de protección deben centrarse en garantizar que el mensaje resulte ininteligible a nuestro atacante.

- Alteraciones en el mensaje. Este problema puede llegar a ser mucho peor que el anterior, ya que si recibimos un mensaje que ha sido modificado y lo damos por bueno, las consecuencias para la comunicación pueden ser catastróficas. En este

sentido, las alteraciones pueden aplicarse tanto sobre el mensaje propiamente dicho, como sobre la información acerca de su verdadera procedencia.

La Criptografía, como ya hemos visto en anteriores capítulos, proporciona mecanismos fiables para evitar los dos peligros que acabamos de mencionar. En general, cada una de las aplicaciones concretas que necesiten de estas técnicas poseerá unas características específicas, por lo que en cada caso habrá una combinación de algoritmos criptográficos que permitirá proporcionar al sistema el nivel de seguridad necesario. Estas combinaciones de algoritmos se estructurarán finalmente en forma de protocolos, para proporcionar métodos de comunicación segura normalizados.

16.2. Protocolos TCP/IP

El conjunto básico de protocolos sobre los que se construye la red Internet se conoce popularmente como TCP/IP, agrupación de los nombres de dos de los elementos más importantes, que no los únicos, de la familia: TCP *(Transmission Control Protocol)* e IP *(Internet Protocol)*.

El modelo de comunicaciones sobre el que se basa Internet se estructura en forma de *capas* apiladas, de manera que cada una de ellas se comunica con las capas inmediatamente superior e inferior, logrando diversos niveles de abstracción, que permiten intercambiar información de forma transparente entre ordenadores. La consecuencia más importante de este enfoque es que dos dispositivos cualesquiera, que pueden estar conectados a Internet por medios totalmente distintos —fibra óptica, cable de cobre, láser, ondas electromagnéticas...—, y separados por multitud de enlaces diferentes —satélite, cables submarinos, redes inalámbricas...—, pueden conectarse entre ellos simplemente con que dispongan de una implementación de TCP/IP.

A diferencia del modelo OSI, que consta de siete capas, denominadas *aplicación, presentación, sesión, transporte, red, enlace* y *física*, los protocolos TCP/IP se organizan únicamente en cinco (figura 16.1). Aunque la correspondencia no es exacta, podemos decir que, básicamente, los tres niveles superiores del modelo OSI se agrupan en el nivel de aplicación de TCP/IP. Comentaremos brevemente cada uno de ellos:

- *Capa Física*. Describe las características físicas de la comunicación, como son el medio empleado, los voltajes necesarios, la modulación empleada, etc.
- *Capa de Enlace*. Indica cómo los paquetes de información viajan a través del medio físico, indicando qué campos de bits se añaden a éstos para que puedan ser reconocidos satisfactoriamente en destino. Ejemplos de protocolos de enlace: Ethernet, 802.11 WiFi, Token Ring, etc.

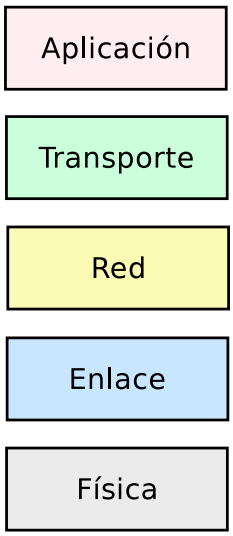

Figura 16.1: Esquema del conjunto de protocolos TCP/IP, en los que se basa la red Internet.

- *Capa de Red*. En ella se ubica el protocolo IP, cuyo propósito consiste en hacer llegar los paquetes a su destino a través de una única red. Existen algunos protocolos de mayor nivel, como ICMP o IGMP, que aunque se construyen sobre IP, también pertenecen a la capa de red, a diferencia de lo que ocurre en el modelo OSI.

- *Capa de Transporte*. Su propósito es garantizar que los paquetes han llegado a su destino, y en el orden correcto. El protocolo más importante en este nivel es TCP, pero existen otros como UDP, DCCP o RTP.

- *Capa de Aplicación*. Esta es la capa a la que acceden de forma directa la mayoría de las aplicaciones que usan Internet. En ella se reciben los datos, que son pasados a las capas inferiores para que sean enviados a su destino. A este nivel pertenecen prococolos tales como HTTP, FTP, SSH, HTTPS, IMAP, DNS, SMTP, IRC, etc.

En la práctica, podemos encontrar protocolos encaminados a obtener comunicaciones seguras en prácticamente todos los niveles de este esquema. En las próximas secciones comentaremos brevemente algunos de ellos.

Los distintos protocolos de comunicación segura pueden ser utilizados para construir las denominadas redes privadas virtuales. Una red privada virtual, en inglés

VPN *(Virtual Private Network)* es una red de comunicaciones privada construida sobre una red pública. Hacia los usuarios se comporta como si de una red interna se tratase, ofreciendo acceso únicamente a aquellos que estén autorizados, y resultando inaccesible para los demás, cuando en realidad todas las conexiones se realizan a través de Internet.

16.3. Protocolo SSL

El protocolo SSL (*Secure Sockets Layer*), desarrollado originalmente por la empresa Netscape, permite establecer conexiones seguras a través de Internet, de forma sencilla y transparente. Se sitúa en la capa de aplicación (figura 16.1), directamente sobre el protocolo TCP, y aunque puede proporcionar seguridad a cualquier aplicación que corra sobre TCP, se usa principalmente para proporcionar seguridad a los protocolos HTTP *(web)*, SMTP *(email)* y NNTP *(news)*, dando lugar en el primero de los casos a los servidores *web* seguros, cuya URL comienza por el prefijo `https://`. Su fundamento consiste en interponer una fase de codificación de los mensajes antes de enviarlos a través de la red. Una vez que se ha establecido la comunicación, cuando una aplicación quiere enviar información a otra computadora, la capa SSL la recoge y la codifica, para luego enviarla a su destino a través de la red. Análogamente, el módulo SSL del otro ordenador se encarga de decodificar los mensajes y se los pasa como texto claro a la aplicación destinataria.

SSL también incorpora un mecanismo de autentificación que permite garantizar la identidad de los interlocutores. Típicamente, ya que este protocolo se diseñó originalmente para establecer comunicaciones *web*, el único que suele autentificarse es el servidor, aunque también puede realizarse una autentificación mutua.

Una comunicación a través de SSL implica tres fases fundamentalmente:

- Establecimiento de la conexión y negociación de los algoritmos criptográficos que van a usarse en la comunicación, a partir del conjunto de algoritmos soportados por cada uno de los interlocutores.
- Intercambio de claves, empleando algún mecanismo de clave pública (ver sección 12.4.1), y autentificación de los interlocutores a partir de sus certificados digitales (ver capítulo 17).
- Cifrado simétrico del tráfico.

Una de las ventajas de emplear un protocolo de comunicaciones en lugar de un algoritmo o algoritmos concretos, es que ninguna de las fases del protocolo queda

atada a ningún algoritmo, por lo que si en el futuro aparecen algoritmos mejores, o alguno de los que se emplean en un momento dado quedara comprometido, el cambio se puede hacer sin modificar el protocolo. En la actualidad, las implementaciones típicas de SSL soportan algoritmos como RSA, Diffie-Hellman o DSA para la parte asimétrica (capítulo 12); RC2, RC4, IDEA, DES, TripleDES o AES para la simétrica (capítulos 10 y 11), y como funciones resumen (capítulo 13) SHA-1 o MD5.

Las ventajas de SSL son evidentes, ya que liberan a las aplicaciones de llevar a cabo las operaciones criptográficas antes de enviar la información, y su transparencia permite usarlo de manera inmediata sin modificar apenas los programas ya existentes. Desde hace tiempo los principales navegadores de Internet incorporan un módulo SSL, que se activa de forma automática cuando es necesario. Hasta diciembre de 1999, debido a las restricciones de exportación de material criptográfico existentes en los EE.UU., la mayoría de los navegadores incorporaban un nivel de seguridad bastante pobre (claves simétricas de 40 bits), por lo que conviene comprobar qué nivel de seguridad se está empleando cada vez que hagamos una conexión.

Existen implementaciones de SSL que permiten construir los denominados *túneles SSL*, que permiten dirigir cualquier conexión a un puerto TCP a través de una conexión SSL previa, de forma transparente para las aplicaciones que se conectan.

16.4. Protocolo TLS

TLS (descrito en el documento *RFC 2246*) es un protocolo basado en la versión 3.0 de SSL, si bien con una serie de mejoras que lo hacen incompatible con este último. Una de las ventajas que proporciona sobre SSL es que puede ser *iniciado* a partir de una conexión TCP ya existente, lo cual permite seguir trabajando con los mismos puertos que los protocolos no cifrados. Mientras que SSL es un protocolo incompatible con TCP, lo cual significa que no podemos establecer una conexión de un cliente TCP a un sevidor SSL ni al revés, y por tanto es necesario diferenciarlos utilizando distintos números de puerto (80 para un servidor *web* normal y 443 para un servidor *web* sobre SSL), con TLS puede establecerse la conexión normalmente a través de TCP y el puerto 80, y luego activar sobre el mismo el protocolo TLS.

En este protocolo se emplea una serie de medidas de seguridad adicionales, encaminadas a protegerlo de distintos tipos de ataque, en especial de los de intermediario (sección 12.2):

- Uso de funciones MAC en lugar de funciones MDC únicamente (ver capítulo 13).

- Numeración secuencial de todos los campos que componen la comunicación, e incorporación de esta información al cálculo de los MAC.
- Protección frente a ataques que intentan forzar el empleo de versiones antiguas —menos seguras— del protocolo o cifrados más débiles.
- El mensaje que finaliza la fase de establecimiento de la conexión incorpora una signatura *(hash)* de todos los datos intercambiados por ambos interlocutores.

Si bien el método usado con más frecuencia para establecer conexiones seguras a través de Internet sigue siendo SSL, cabe esperar que con el tiempo sea paulatinamente reemplazado por TLS, y que este último se convierta en el estándar de seguridad para las comunicaciones cifradas en Internet.

16.5. Protocolos IPsec

IPsec es un estándar que proporciona cifrado y autentificación a los paquetes IP, trabajando en la capa de red (figura 16.1). En lugar de tratarse de un único protocolo, IPsec es en realidad un conjunto de protocolos, definidos en diversos *RFC*s (principalmente en el 2401), encaminados a proporcionar autentificación, confidencialidad e integridad a las comunicaciones IP. Su carácter obligatorio dentro del estándar IPv6 —recordemos que en IPv4, la versión más empleada en la actualidad de este protocolo, es opcional— hará con seguridad que la popularidad de IPsec crezca al mismo ritmo que la implantación de la nueva versión del protocolo IP.

IPsec puede ser utilizado para proteger una o más rutas entre un par de ordenadores, un par de *pasarelas de seguridad* —ordenadores que hacen de intermediarios entre otros, y que implementan los protocolos IPsec— o una pasarela y un ordenador. En función del tipo de ruta que se proteja, se distinguen dos modos de operación:

- *Modo túnel*: Se realiza entre dos pasarelas de seguridad, de forma que éstas se encargan de crear una ruta segura entre dos ordenadores conectados a ellas, a través de la cual viajan los paquetes. De este modo se puede disponer dentro de una red local de un ordenador que desempeñe las labores de pasarela, al que las computadoras de la propia red envíen los paquetes, para que éste les aplique los protocolos IPsec antes de remitirlos al destinatario —o a su pasarela de seguridad asociada—. Este modo permite interconectar de forma segura ordenadores que no incorporen IPsec, con la única condición de que existan pasarelas de seguridad en las redes locales de cada uno de ellos.

- *Modo transporte*: En este caso los cálculos criptográficos relativos a los protocolos IPsec se realizan en cada extremo de la comunicación.

Básicamente, IPsec se compone a su vez de dos protocolos, cada uno de los cuales añade una serie de campos, o modifica los ya existentes, a los paquetes IP:

- Cabecera de autentificación IP, abreviado como AH *(IP Authenticacion Header)*, diseñado para proporcionar integridad, autentificación del origen de los paquetes, y un mecanismo opcional para evitar ataques por repetición de paquetes.

- Protocolo de encapsulamiento de carga de seguridad, o ESP *(Encapsulating Security Payload)* que, además de proveer integridad, autentificación y protección contra repeticiones, permite cifrar el contenido de los paquetes.

Debido a que algunos de los servicios que IPsec proporciona necesitan de la distribución e intercambio de las claves necesarias para cifrar, autentificar y verificar la integridad de los paquetes, es necesario que éste trabaje en consonancia con un conjunto externo de mecanismos que permita llevar a cabo esta tarea, tales como IKE, SKIP o Kerberos.