Seguridad en las redes de computadoras

8.1 ¿Qué es la seguridad de red?

Hay que tener ciertas propiedades deseables para tener una comunicacion segura:

- **confidencialidad**: Solo el emisor y el receptor deseado deberán comprender el contenido de los mensajes transmitidos.Es absolutamente necesario que los mensajes sean cifrados
- **Integridad de los mensajes**: El contenido de sus comunicaciones no se vea alterado durante la transmisión
- **Autenticación del punto terminal:** Tanto el emisor como el receptor deberán poder confirmar la identidad del otro en el proceso de comunicación
- **Seguridad operacional:** detector de intrusos o firewalls.

Un intruso puede potencialmente
- Curiosear (husmear y registrar los mensajes de control y de datos que se transmiten por el canal).
- Modificar, insertar o borrar mensajes o el contenido de los mismos.

Estás capacidades permitirán a un intruso hacer una variedad de ataques contra la seguridad de la red como escuchando las comunicaciones, suplantando a otra entidad, denegando el servicio a usuarios legitimos.

8.2 Principios de la criptografía

Las técnicas criptográficas permiten a un emisor **ocultar los datos** de modo que los intrusos **no puedan obtener ninguna información** a partir de los datos interceptados. El receptor, por supuesto, deberá ser capaz de recuperar los datos originales a partir de los datos ocultados.

La propia técnica de cifrado es conocida, en el sentido de que es pública, está estandarizada y está disponible para todo el mundo incluso para los potenciales intrusos. Hay una forma para impedir describrar los datos transmitidos: **accion de claves**
Cuando se tiene un mensaje y se quiere encriptar **se proporciona una clave** que puede ser una cadena de numeros o caracteres como entrada para el algoritmo de cifrado. El algoritmo de cifrado toma la clave KA y el mensaje de texto en claro, como entrada y genera el texto cifrado como salida.

De la misma forma se proporciona una clave KB al algoritmo de descifrado que toma el texto cifrado y la clave KB como entrada y genera como salida el texto en claro original.

Entonces si tenes q benito recibe un mensaje cifrado KA(m) el para descifrarlo aplica KB(KA(m))

8.2.1 Criptografía de clave simétrica

Ambas claves de cifrado y descifrado son las mismas.

Todos los algoritmos criptográficos implican sustituir una cosa por otra; por ejemplo, se toma un fragmento de texto en claro y luego se calcula y sustituye por el texto cifrado apropiado para crear el mensaje cifrado.

Un algoritmo de clave simétrica muy simple y muy antiguo es el cifrado de César, donde se toma cada letra del mensaje en claro y sustituyéndola por la letra que está k posiciones por detrás en el alfabeto. Una mejora es el cifrado monoalfabético, donde cualquier letra puede sustituirse por cualquier otra.

Hay 3 escenarios distintos para ver lo fácil que se puede romper el esquema de un cifrado:

- **Ataque de sólo texto cifrado**: es cuando el intruso puede tener acceso únicamente al texto cifrado interceptado, donde el tener análisis estadístico puede ayudar a realizar este ataque.
- **Ataque de texto en claro conocido:** Es cuando un intruso conoce algunas de las parejas de letras (texto en claro, text cifrado).
- **Ataque de texto en claro seleccionado:**el intruso tiene la posibilidad de elegir el mensaje de texto en claro y obtener su correspondiente texto cifrado**.**

Luego se inventó el **cifrado polialfabético**, que permitía mejorar el cifrado monoalfabético. La idea subyacente al cifrado polialfabético es utilizar varios cifrados monoalfabéticos, utilizando un cifrado monoalfabético específico para codificar cada letra
situada en una posición específica dentro del mensaje de texto en claro. De ese modo, una misma letra que aparezca en diferentes posiciones dentro del mensaje en claro se podría codificar de forma distinta cada vez.

Existen dos clases generales de técnicas de cifrado simétrico: cifrados de flujo y cifrados de bloque.

Cifrados de bloque

En un cifrado de bloque, el mensaje que hay que cifrar se procesa en bloques de k bits. Por ejemplo, si k 5 64, entonces el mensaje se descompone en bloques de 64 bits y cada bloque se cifra de forma independiente.

Encadenamiento de bloques cifrados

En las aplicaciones de redes de computadoras, normalmente es necesario cifrar mensajes de gran tamaño. Si se aplicara el cifrado en bloques ocurre el problema de que dos o más bloques de texto en claro podrian ser identicos y bajo este mecanismo se produciria el mismo texto cifrado. Para resolver este problema se puede incluir cierta **aleatoriedad** en el texto de cifrado de modo que idénticos bloques de texto en claro produzcan bloques de texto cifrado diferentes.

El introducir **la aleatoriedad** resuelve un problema pero crea otro: ahora se tiene que **transmitir el doble de bits** que antes. Por cada bit de cifrado, ahora debe ahora enviar también un bit aleatorio, **duplicando así el ancho de banda requerido.**

Lo que se suele aplicar es una técnica denominada **encadenamiento de bloques cifrados** (CBC). La idea básica consiste en **enviar sólo un valor aleatorio** junto con el primer mensaje, y hacer que el

emisor y el receptor utilicen los bloques codificados calculados, en lugar de los subsiguientes números aleatorios.

Cómo funciona:

1. Antes de cifrar el mensaje, el emisor genera una cadena aleatoria de k bits, denominada vector de inicialización (IV) y lo envía sin cifrar.
2. El emisor calcula calcula la operación OR exclusiva del primer bloque de texto en claro con IV. Luego pone el resultado en el algoritmo de cifrado de bloque para obtener el bloque de texto cifrado. El emisor envía al receptor.
3. Para el i-ésimo bloque, el emisor genera el i-ésimo bloque de texto cifrado

Consecuencias:

- El receptor continuará pudiendo recuperar el mensaje original.
- Incluso si dos bloques de texto en claro son idénticos, los textos cifrados correspondientes serán (casi siempre) diferentes
- aunque el emisor envíe el vector IV sin cifrar, ningún intruso podrá descifrar los bloques de texto cifrado dado que no conocen la clave secreta
- Poco incremento de ancho de banda al solo enviar un bloque de sobrecarga

8.2.2 Cifrado de clave pública

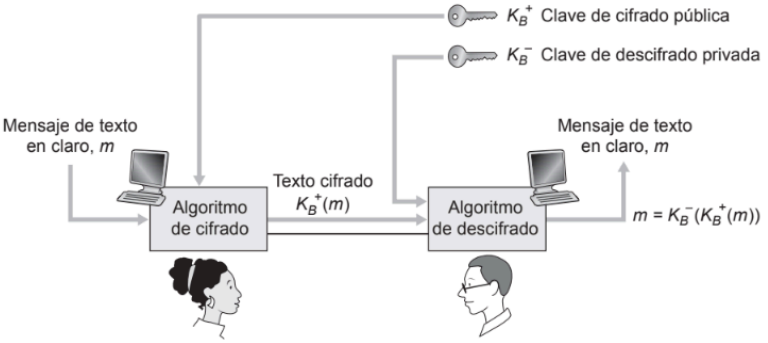
Una clave pública que está disponible para todo el mundo. El sender primero obtiene la clave pública del receiver y la utiliza para encriptar el mensaje. El receiver lo desencripta utilizando la clave privada.

Obviamente, para que la criptografía de clave pública pueda funcionar, **la selección de claves** y el **cifrado/descifrado** deben hacerse de forma tal que sea imposible para un intruso determinar la clave privada de Benito o descifrar o adivinar de alguna otra manera el mensaje que Alicia le ha enviado a Benito.

Ademas se necesita de una firma digital para poder enviar un mensaje cifrado a una persona utilizando su clave públicamente.

RSA

Este algortimo se ha convertido casi en sinonimo de la criptografia de clave pública.
RSA hace un extenso uso de las operaciones aritméticas módulo n.



En RSA existen dos componentes interrelacionados:

- La elección de las claves pública y privada.
- El algoritmo de cifrado y descifrado

Para generar las claves RSA pública y privada se utilizan números primos grandes, p y q (cuanto más grandes más dificl será romper el algoritmo pero tarda en realizar la codificación y decodificacion) y se hacen calculos de multiplicacion y division.

COMO SE USA: yo tengo que cifrar el mensaje con la clave pública del receptor + un algoritmo de cifrado conocido. El receptor, va a utilizar su clave privada + el algoritmo de cifrado conocido para descifrar.

Claves de sesion

RSA se utiliza en la práctica en combinación con algún otro mecanismo criptográfico de clave simétrica.

Primero se elegiría una clave para codificar los propios datos; esta clave se conoce como **clave de sesión**. Alicia tiene que comunicar a Benito la clave de sesión, ya que se trata de la clave simétrica compartida que ambos utilizarán con un sistema de cifrado de clave simétrica.

Alicia cifra la clave de sesión utilizando la clave pública de Benito, Benito recibe la clave de sesión cifrada mediante RSA, c, y la descifra para obtener la clave de sesión

De este modo, ahora Benito conoce la clave de sesión que Alicia emplea para transferir los datos cifrados.

¿Por qué funciona RSA? La seguridad del algoritmo RSA se basa en el hecho de que no existen algoritmos conocidos para factorizar rápidamente un número, en este caso el valor público n, con el fin de obtener los números primos p y q. Tampoco se sabe si existen algoritmos rapidos para factorizar un número. Es por eso que con RSA la seguridad no está garantizada.

8.3 Integridad de los mensajes y firmas digitales

8.3.1 Funciones hash criptográficas

Se necesita un hash el cual sea inviable para un intruso reemplazar el mensaje por otro que tenga aplicado el mismo hash.
El checksum, por ejemplo, es malísimo porque es fácil encontrar otro mensaje que de igual checksum. Algunos de los algoritmos más usados actualmente son MD5 y SHA-1.

8.3.2 Código de autenticación del mensaje

Para garantizar la integridad de los mensajes, además de utilizar funciones hash criptográficas Alicia y Benito necesitan un secreto compartido. Este secreto compartido, que no es más que una cadena de bits, se denomina clave de autenticación.

Alicia crea el mensaje m, concatena s con m para crear m 1 s y calcula el valor hash H(m+s) (por ejemplo con SHA-1). H(m+s) se denomina código de autenticación de mensajes (**MAC**, Message Authentication Code).

Utilizando un código MAC, las entidades pueden autenticar los mensajes que se intercambian sin tener que incluir complejos algoritmos de cifrado en el proceso de garantía de la integridad.

El administrador puede distribuir la clave de autenticación a cualquiera de los routers cifrándola con la clave pública del router y luego enviando la clave cifrada hasta el router a través de la red.

8.3.3 Firmas digitales

Las firmas digitales deben realizarse de forma que sean verificables y no falsificables. Con la criptografía de clave pública, Benito dispone de sendas claves pública y privada, siendo la pareja formada por esas claves distintivas de Benito.

- Quienquiera que haya firmado el documento tiene que haber utilizado la clave privada, K_B^- , para calcular la firma $K_B^-(m)$, tal que $K_B^+(K_B^-(m)) = m$.
- La única persona que puede conocer la clave privada, K_B^- , es el propio Benito. Recuerde, de

las firmas digitales también proporcionan un mecanismo de integridad de los mensajes, permitiendo al receptor verificar que el mensaje no ha sido alterado, además de verificar el origen del mismo.

Uno de los problemas con la firma de datos mediante mecanismos de cifrado es que el cifrado y el descifrado son computacionalmente muy caros. Una técnica más eficiente consiste en introducir funciones hash en el mecanismo de firma digital.

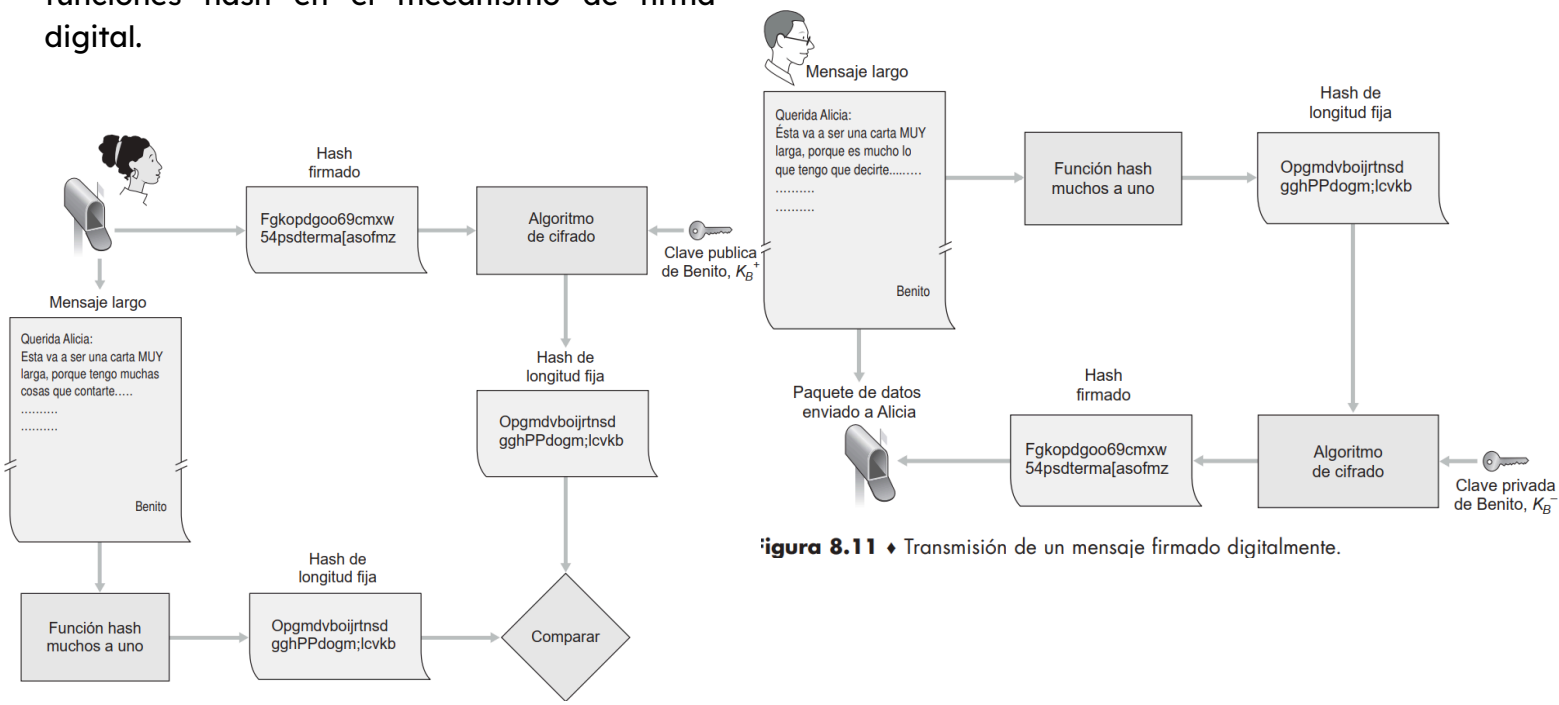


Figura 8.11 ♦ Transmisión de un mensaje firmado digitalmente.

Certificación de clave pública

Se tiene que certificar que una clave pública pertenece a una entidad específica.
La asociación entre una clave pública y una entidad la realiza una Autoridad de certificación (CA, Certification Authority), cuyo trabajo consiste en validar las identidades y emitir los certificados que asocian con esa entidad su correspondiente clave pública.

8.4 Autenticación del punto terminal

La autenticación del punto terminal es el proceso de demostrar a alguien la propia identidad a través de una red de computadoras. La autenticación debe realizarse basándose exclusivamente en los mensajes y datos intercambiados como parte de un protocolo de autenticación.

por qué se proporciona la funcionalidad de seguridad en más de una capa dentro de Internet. ¿No bastaría simplemente con proporcionar la funcionalidad de seguridad en la capa de red? Aunque la seguridad en la capa de red puede proporcionar la funcionalidad básica de cifrado de todos los datos contenidos en los datagramas y de autenticar todas las direcciones IP de origen, lo que no puede es ofrecer seguridad de nivel
de usuario. Por ejemplo, un sitio web de comercio electrónico no puede confiar en la seguridad de la capa IP para autenticar a un cliente que esté comprando bienes o servicios en ese sitio. Por tanto, existe una necesidad de incorporar funcionalidad de seguridad en las capas superiores, además de la funcionalidad básica en las capas inferiores. En segundo lugar, es más fácil generalmente implantar servicios Internet nuevos, incluyendo los servicios de seguridad, en las capas superiores de la pila de protocolos.

8.5.2 Pretty Good Privacy (PGP)

es un buen ejemplo de esquema de cifrado de correo electrónico

Cuando se instala PGP, el software crea una pareja de clave pública y clave privada para el usuario. La clave pública puede darse a conocer a todo el mundo a través del sitio web del usuario o puede almacenarse en un servidor de clave pública. La clave privada está protegida mediante el uso de una contraseña. La contraseña debe introducirse cada vez que el usuario accede a la clave privada. PGP le da al usuario la opción de firmar digitalmente el mensaje, de cifrar el mensaje o de realizar tanto la operación de firma como la de cifrad

8.6 Asegurando las conexiones TCP: SSL

SSL (Secure Sockets Layer) se utiliza para asegurar conexiones TCP. Provee confidencialidad, integridad de los datos, autenticación de cliente y servidor.

Puede verificar que su navegador está usando SSL viendo si el URL comienza por https. Puede ser empleado por cualquier aplicación que se ejecute sobre TCP.
SSL se compone de 3 fases:

Fase de acuerdo

Una vez que se ha establecido la conexión TCP, Benito envía a Alicia un mensaje de saludo.

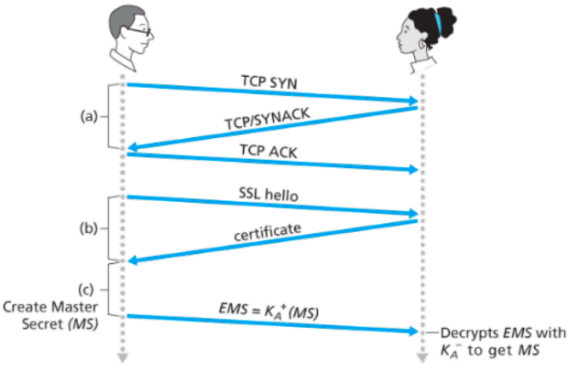


Figure 8.25 The almost-SSL handshake, beginning with a TCP connection

En el **handshake** se establece la conexión TCP, se verifica que el servidor sea realmente el servidor y se le envía al servidor una **clave secreta** que van a usar cliente-servidor para generar las claves simétricas.
En **SSL posta** durante el handshake se puede **acordar el algoritmo criptográfico**. Además, durante el handshake ambas partes **se envían nonces** que se van a usar para la **deducción de claves**.

1. El cliente envía la lista de algoritmos criptográficos que soporta, junto con un número distintivo de cliente.
2. A partir de la lista, el servidor e**lige un algoritmo simétrico, un algoritmo de clave pública** (por ejemplo, RSA) y un algoritmo **MAC**. Devuelve al cliente las elecciones, un certificado y un número distintivo de servidor.
3. El cliente **verifica el certificado, extrae la clave pública del servido**r, genera una clave premaestra (PMS, Pre-Master Secret), cifra la PMS con la clave pública del servidor y envía la PMS cifrada al servidor.
4. Utilizando la misma función de deducción de clave (como la especificada por el estándar SSL), el cliente y el servidor calculan independientemente la clave maestra (MS) a partir de la PMS y de los números distintivos. La MS se divide entonces para generar las dos claves de cifrado y las dos claves MAC. Además, cuando el cifrado simétrico elegido emplea CBC (tal como 3DES o AES) también se obtienen a partir de la MS dos vectores de inicialización (IV), uno para cada lado de la conexión. A partir de este momento todos los mensajes intercambiados entre el cliente y el servidor son cifrados y autenticados (con un código MAC).
5. El cliente envía un código MAC de todos los mensajes de acuerdo.
6. El servidor envía un código MAC de todos los mensajes de acuerdo.

Los números distintivos se emplean para defenderse de los **"ataques por reproducción de la conexión"**, mientras que los números de secuencia se emplean para defenderse frente a la reproducción de paquetes individuales durante una sesión activa.

Deducción de las claves

se considera más seguro que Alicia y Benito utilicen claves criptográficas distintas y también que empleen claves distintas para el cifrado y las comprobaciones de integridad.
Tanto Alicia como Benito utilizan **la clave maestra** para **generar cuatro claves**:

1. Eb = **Clave de cifrado** de sesión para los datos que Benito envía a Alicia
2. Ea = clave de cifrado de sesión para los datos que Alicia envía a Benito
3. Mb = **clave MAC** de sesión para los datos que Benito envía a Alicia
4. Ma = clave MAC de sesión para los datos que Alicia envía a Benito.

Las dos claves de cifrado se utilizarán para cifrar los datos y las dos claves MAC se emplearán para verificar la integridad de los datos.

Transferencia de datos

SSL divide el flujo de datos en registros, añade un código MAC a cada registro para comprobar la integridad y luego cifra (con clave de cifrado de sesión E_B) el registro junto con el código MAC. Para crear el valor MAC'se hashem los datos del registro y la clave M_B.

Este paquete cifrado se pasa entonces a TCP para transportarlo a través de Internet
Suponiendo que cada segmento TCP encapsula exactamente un registro, vamos a ver ahora cómo procesaría Alicia dichos segmentos:

1. El TCP que se ejecuta en Alicia pensará que todo es correcto y pasará los dos registros a la subcapa SSL.
2. SSL en Alicia descifrará los dos registros.

3. SSL en Alicia utilizará la clave MAC en cada registro para verificar la integridad de los datos de los dos registros.
4. SSL pasaría a continuación los flujos de bytes descifrados de los dos registros a la capa de aplicación; pero el flujo de bytes completo recibido por Alicia no estaría en el orden correcto debido a la inversión del orden de los registros.

¿Cómo se soluciona el orden?

Benito mantiene un contador de número de secuencia, que se inicializa en cero y que se incrementa cada vez que envía un registro SSL. Benito cuando calcula el código MAC incluye el número de secuencia en el cálculo del código MAC. Así, ahora el valor **MAC es un hash de los datos más la clave MAC M_B más el número de secuencia actual**.
Alicia controla los números de secuencia de Benito, pudiendo verificar la integridad de los datos de un registro incluyendo el número de secuencia apropiado en el cálculo de MAC

Cierre de la conexión

Consiste en indicar en el **campo de tipo si el registro sirve para terminar la sesión SSL**. Así, si Alicia recibiera un segmento TCP FIN antes de recibir un registro SSL de cierre deducirá inmediatamente que algo raro está sucediendo.

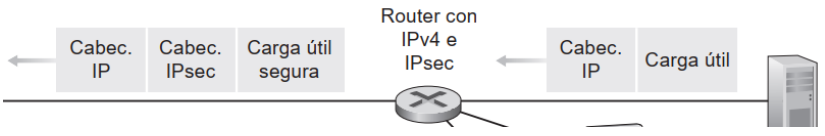
8.7 Seguridad de la capa de red: IPsec y redes privadas virtuales

VPN

Red privada: Red física independiente (incluyendo routers, enlaces y una infraestructura DNS) que esté **completamente separada de la red Internet pública**. De modo que sus hosts y servidores puedan intercambiarse datos de forma segura y confidencial.

IPsec asegura datagramas entre dos entidades cualquiera de capa de red. Muchas instituciones lo usan para crear VPNs (virtual private networks). **Provee confidencialidad, mecanismos para la integridad, autenticación y prevención de ataques** de tipo replay.

Cuando un host de la oficina principal envía un datagrama IP el router de pasarela de la oficina principal **convierte el datagrama IPv4 en un datagrama IPsec** y luego lo reenvía hacia Internet. Este datagrama IPsec tiene una cabecera IPv4 tradicional, de modo que los routers de la red Internet pública **procesan el datagrama como si se tratara de un datagrama IPv4** normal -> la carga útil del datagrama IPsec está cifrada



Cuando el datagrama IPsec llega al receptor, descifra la carga útil y proporciona otros servicios de seguridad, como la **verificación de la integridad de los datos**, y pasa la carga útil descifrada hacia el protocolo de la capa de transporte

En la serie de protocolos IPsec hay dos protocolos principales:

- AH, Authentication Header: Proporciona autenticación del origen, integridad de los datos

- **ESP**, Encapsulation Security Payload: Proporciona **autenticación del origen**, **integridad de los datos** y **confidencialidad**.

8.7.3 Asociaciones de seguridad

Antes de enviar datagramas IPsec, ambas entidades crean una conexión lógica unidireccional en la capa de red: asociación de seguridad (SA, Security Association).
Si ambas entidades desean enviarse datagramas seguros entre sí, entonces será necesario establecer 2 SA

Cada entidad IPsec (router o host) suele mantener información de estado para muchas asociaciones de seguridad y la almacena en una db

8.7.4 El datagrama IPsec

IPsec tiene dos formas distintas de paquete, una para el denominado modo túnel y otra para el denominado modo transporte (Solo vamos a estudiar modo tunel)

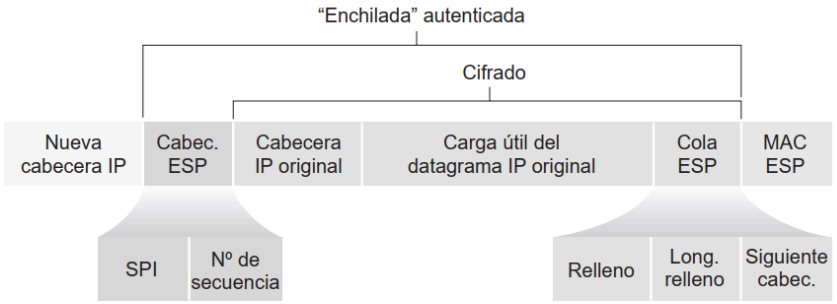


Figura 8.29 ♦ Formato del datagrama IPsec.

la carga útil contiene una cabecera ESP, el datagrama IP original, una cola ESP y un campo de autenticación
ESP (estando cifrados el datagrama original y la cola ESP)
Puesto que el datagrama IPsec incluye el datagrama IP original, estas direcciones se incluyen (y se cifran) como parte de la carga útil del paquete IPsec

Cómo opera el receptor:

1. Analizando la enchilada, R2 utiliza el SPI para determinar a qué asociación de seguridad (SA) pertenece el datagrama.
2. Calcula el valor MAC de la enchilada y verifica que es coherente con el valor contenido en el campo ESP MAC. Si lo es, el router sabrá que la enchilada procede del router R1 y que no ha sido manipulada.
3. Comprueba el campo de número de secuencia para verificar que el datagrama sea reciente y no un datagrama reproducido.
4. Descifra la unidad cifrada utilizando la clave y el algoritmo de descifrado asociados con la SA.
5. Elimina el relleno y extrae el datagrama IP normal original.
6. Reenvía el datagrama original a la red de la sucursal para que el datagrama llegue a su verdadero destino.

Junto con una base de datos SAD, la entidad IPsec también mantiene otra estructura de datos denominada base de datos de políticas de seguridad (SPD, Security Policy Database). La SPD indica

qué tipos de datagramas (en función de la dirección IP de origen, la dirección IP de destino y el tipo de protocolo) hay que procesar mediante IPsec; y para aquellos que haya que procesar mediante IPsec, qué SA debe emplearse

Resumen de los servicios IPsec

¿Qué servicios proporciona IPsec exactamente?
Un atacante no puede ver el datagrama original. De hecho, no solo están los datos del datagrama original ocultos y también lo están el número de protocolo, la dirección IP de origen y la dirección IP de destino.
Para los datagramas enviados a través de la SA, solo se sabe que el datagrama tiene su origen en algún host de la red 172.16.1.0/24 y que está destinado a algún host de la red 172.16.2.0/24. N**o sabe si está transportando datos TCP, UDP o ICMP**; **no sabe si está transportando HTTP, SMTP**, o algún otro tipo de datos de aplicación. Esta confidencialidad, por tanto, va bastante más allá que en SSL.
En segundo lugar, suponga que un atacante trata de alterar un datagrama en la SA modificando algunos de sus bits. Cuando este datagrama alterado llegue a R2 no pasará las comprobaciones de integridad (utilizando el valor MAC)
En tercer lugar, el atacante intenta hacerse pasar por R1, creando un datagrama IPsec cuyo origen sea 200.168.1.100 y cuyo destino sea 193.68.2.23. El ataque no tendrá ningún efecto, ya que este datagrama de nuevo no pasará la comprobación de integridad realizada en R2. Finalmente, puesto que IPsec incluye números de secuencia, no se podrá desarrollar con éxito ningún ataque por reproducción.

En resumen IPsec proporciona (entre cualquier pareja de dispositivos que procesen paquetes en la capa de red) **mecanismos de confidencialidad, de autenticación del origen, de integridad de los datos y de prevención de los ataques por reproducción**.

8.8 Asegurando las redes LAN inalámbricas

8.8.1 WEP (Wired Equivalent Privacy)

El protocolo WEP fue diseñado para proporcionar **autenticación** y **cifrado** de datos entre un host y un punto de **acceso inalámbrico** (es decir, una estación base) utilizando una técnica basada en una **clave simétrica compartida.**
Se presupone que el host y el punto de acceso inalámbrico acuerdan qué clave utilizar, empleando para ello algún método fuera de banda.

La autenticación se lleva a cabo de la forma siguiente:

1. Un host inalámbrico solicita la autenticación al punto de acceso.
2. El punto de acceso responde a la solicitud de autenticación con un número distintivo (nonce)
3. **El host inalámbrico cifra el número distintivo utilizando la clave simétrica**
4. El punto de acceso descifra el número distintivo cifrado por el host.

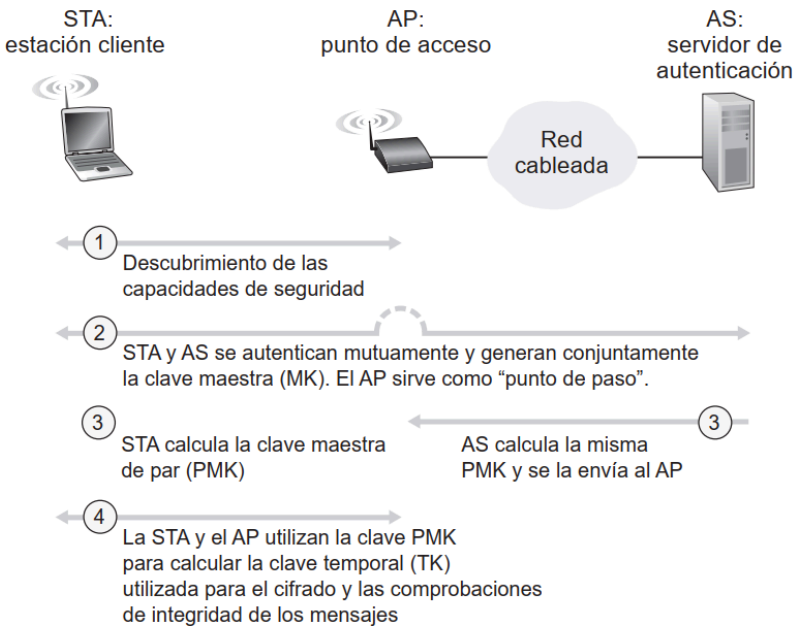
Si el número distintivo descifrado se corresponde con el valor del número distintivo originalmente enviado al host, entonces el host quedará autenticado por el punto de acceso.
la clave WEP cambia de una trama a otra

8.2.2 IEEE 802.11i

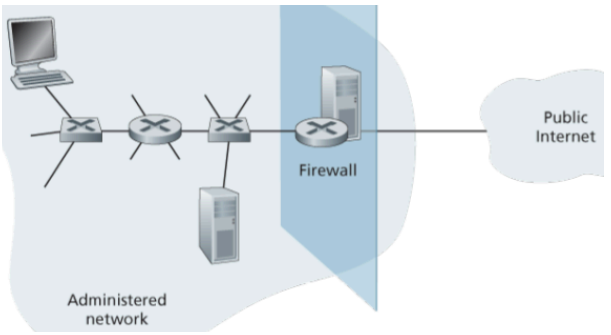
IEEE 802.11i proporciona formas mucho más fuertes de cifrado, un conjunto ampliable de mecanismos de autenticación y un mecanismo de distribución de claves
802.11i define un servidor de autenticación con el que el AP puede comunicarse.
Separar el servidor de autenticación del AP permite que un mismo servidor de autenticación preste servicio a muchos puntos de acceso, centralizando la autenticación y el acceso y manteniendo a un nivel bajo el coste y la complejidad de los puntos de acceso.

802.11i opera en **cuatro fases**:

1. Descubrimiento. En la fase de descubrimiento el AP anuncia su presencia y las formas de autenticación y cifrado, y el cliente solicita
2. Autenticación mutua y generación de la clave maestra MK.
3. Generación de la clave maestra de par (PMK, Pairwise Master Key). La MK es un secreto compartido que solo conocen el cliente y el servidor de autenticación y que ambos emplean para generar una segunda clave, la clave maestra de par (PMK).
4. Generación de la clave temporal PMK: ahora generar claves adicionales que se utilizarán para la comunicación y para el cifrado



8.9 Seguridad operacional: cortafuegos y sistemas de detección de intrusiones



8.9.1 Firewall

Un cortafuegos es una combinación de hardware y software que aísla la red interna de la organización de Internet, permitiendo pasar a algunos paquetes y bloqueando a otros.

Objetivos:

- **Todo el tráfico que va del exterior hacia el interior de la red, y viceversa, pasa a través del cortafuegos.** Este se encuentra en el límite entre la red administrada y el resto de Internet. Aunque las organizaciones de gran tamaño pueden utilizar varios niveles de cortafuegos o cortafuegos distribuidos, colocar un cortafuegos en un único punto de acceso a la red facilita la gestión y el imponer una política de control de acceso.
- **Solo se permite el paso del tráfico autorizado de acuerdo con la política de seguridad local.** Con todo el tráfico de entrada y de salida de la red institucional pasando a través del cortafuegos, este puede restringir el acceso al tráfico autorizado.
- **El firewall no puede ser traspasado**. El propio cortafuegos es un dispositivo conectado a la red. Si no está diseñado o instalado apropiadamente puede verse comprometido, en cuyo

caso solo proporciona una falsa sensación de seguridad (lo que es peor que no disponer de cortafuegos)

Los cortafuegos se implementan frecuentemente en los routers y se controlan de forma remota mediante SDN.

Tres categorías

Filtros de paquetes tradicionales

Examina cada datagrama aisladamente basándose en las reglas especificadas por el administrador. Las reglas de cortafuegos se implementan en los routers.

Estas reglas se pueden basar en:

- Las direcciones IP de origen o de destino.
- El tipo de protocolo especificado en el campo de datagrama IP: TCP, UDP, ICMP, OSPF…
- El puerto de destino y de origen TCP o UDP.
- Los bits indicadores TCP: SYN, ACK, etc.
- El tipo de mensaje ICMP.
- Diferentes reglas para los datagramas que salen y entran en la red.
- Diferentes reglas para las distintas interfaces del router

EJEMPLOS:

Política	Configuración del cortafuegos
Sin acceso web externo.	Eliminar todos los paquetes salientes hacia cualquier dirección IP, puerto 80.
Sin conexiones TCP entrantes, excepto las destinadas al servidor web público de la organización.	Eliminar todos los paquetes TCP SYN entrantes hacia cualquier IP excepto 130.207.244.203, puerto 80.
Impedir que las aplicaciones de radio web consuman el ancho de banda disponible.	Eliminar todos los paquetes UDP entrantes, excepto los paquetes DNS.
Impedir que la red sea utilizada para llevar a cabo un ataque DoS distribuido.	Eliminar todos los paquetes ping ICMP hacia una dirección de "difusión" (por ejemplo, 130.207.255.255).
Impedir que la red sea examinada con Traceroute.	Eliminar todo el tráfico ICMP TTL saliente caducado.

Las reglas de cortafuegos se implementan en los routers mediante listas de control de acceso, teniendo cada interfaz del router su propia lista.

Filtros de paquetes con memoria del estado

Se trackean las conexiones TCP y con ese conocimiento se aplican filtros. Se chequea contra la tabla si un paquete nuevo es parte de una conexión ya establecida
Los filtros con **memoria** del estado almacenan la información de todas las conexiones TCP activas en una tabla de conexiones. Esto es posible porque el cortafuegos puede observar el inicio de una nueva conexión observando un acuerdo en tres fases (SYN, SYNACK y ACK) y puede observar el fin de una conexión cuando ve un paquete FIN para la conexión.

Application gateway

Toman decisiones a partir de application data. Es un servidor por el que tiene que pasar toda la data de aplicaciones.

Desventajas:

- Hace falta una pasarela de aplicación diferente para cada aplicación.
- El rendimiento se verá afectado, dado que todos los datos tendrán que ser reenviados a través de la pasarela.

8.9.2 Sistemas de detección de intrusiones

Para detectar varios ataques se necesita hacer un deep packet inspection, es decir **mirar la data que carga el paquete** más allá de los headers

Un dispositivo que **genera alertas** cuando observe la presencia de tráfico potencialmente malicioso se denomina sistema de detección de intrusiones (**IDS**, Intrusion Detection System).

Un dispositivo que **filtra el tráfico** sospechoso se denomina sistema de **prevención** de intrusiones (**IPS**, Intrusion **Prevention** System).
Los sistemas IDS se pueden clasificar en términos generales en sistemas basados en firma osistemas basados en anomalías.

La primera mantiene una base de datos de firmas de ataques. C**ada firma es un set de reglas pertenecient**es a una actividad de intrusión.
La segunda crea un perfil del tráfico a partir de la observación del tráfico en operaciones normales. Busca paquetes estadísticamente inusuales