Ejercicios Tema 5. Seguridad

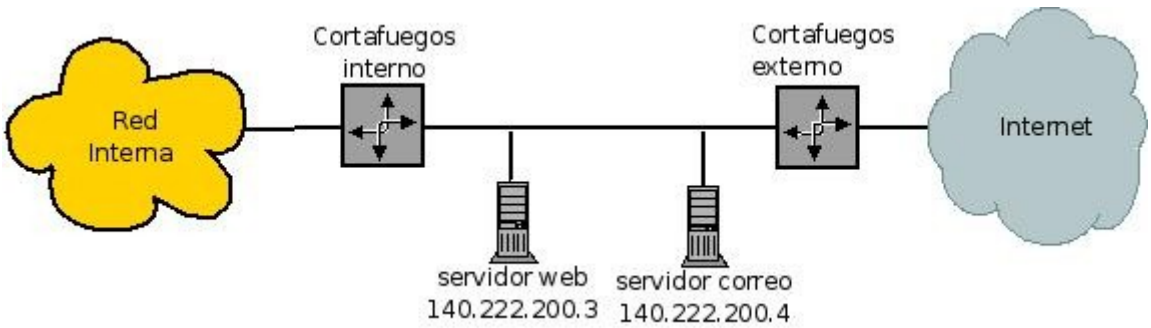
Ej.1. La tabla que tienes a continuación se corresponde con la configuración de un cortafuegos. Revísala e indica qué tráfico externo atravesará el cortafuegos. A tener en cuenta:

a) Dirección de la red protegida por el cortafuegos: 192.168.1.0/24 (en la tabla le falta la máscara).
b) Dirección interna del cortafuegos: 192.168.1.1
c) Dirección del servidor de correo: 192.168.1.2
d) Dirección del servidor web: 192.168.1.3

Contestar en dos casos posibles: 1) que el cortafuegos sea construido sobre Linux mediante iptables, sin haber definido acción por defecto en ninguna cadena, 2) que sea un cortafuegos CISCO mediante ACLs.

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	192.168.1.0	> 1023	Allow	Rule to allow return TCP Connections to internal subnet
2	192.168.1.1	Any	Any	Any	Deny	Prevent Firewall system itself from directly connecting to anything
3	Any	Any	192.168.1.1	Any	Deny	Prevent External users from directly accessing the Firewall system.
4	192.168.1.0	Any	Any	Any	Allow	Internal Users can access External servers
5	Any	Any	192.168.1.2	SMTP	Allow	Allow External Users to send email in
6	Any	Any	192.168.1.3	HTTP	Allow	Allow External Users to access WWW server

Ej.2. Sea una topología como la de la figura, donde se ha establecido una red perimetral en el acceso desde Internet.



Construir una tabla de filtrado para datagramas reenviados en el cortafuegos externo, con las siguientes columnas:

@IP origen	puerto origen	@IP destino	puerto destino	Admitir/Rechazar

Téngase en cuenta:

a) La normativa de seguridad de la red no permite ningún acceso al exterior desde las máquinas de la red interna.
b) El servidor de correo únicamente se conecta a otros servidores SMTP, que, como él, se comunican a través del puerto TCP 25.
c) El servidor web da servicio a través del puerto TCP 80.
d) Consignar de manera explícita una opción por defecto a adoptar en caso de no coincidir con ninguna entrada de la tabla.

Ej.3. ¿Es posible o no el envío del siguiente mensaje en un sistema de cifrado mediante clave pública (suponiendo que no ha habido filtraciones), siendo A el emisor y B el receptor del mensaje M?

Pub_B(Pub_A(Pri_A(Pri_B(M))))

En caso afirmativo, ¿qué se ha enviado? En caso negativo, ¿por qué?

Ej.4. En un sistema de cifrado simétrico, el emisor y el receptor se ponen de acuerdo en el empleo de la primera frase de un determinado libro como clave. Además, también desean verificar la clave, y para ello han ideado el siguiente protocolo:

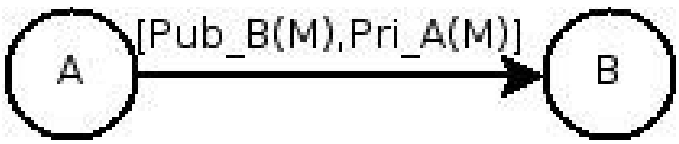
a) Uno genera una secuencia de bits aleatorios, de longitud igual al número de bits de la clave (la primera frase del libro, en ASCII).
b) Con ese número y la clave ejecuta la operación XOR, y envía el resultado al otro.
c) Éste, aplica la función XOR entre lo recibido y la clave, y envía el resultado al primero.
d) El primero verifica si lo recibido coincide con el número por él generado y, en caso afirmativo, considera verificada la clave sin haber sido enviada.

¿Le ves algún inconveniente a este protocolo?

Ej.5. Supongamos que para el establecimiento de una clave de sesión simétrica usamos criptografía asimétrica de la siguiente forma: Una de las dos partes (A) crea la clave simétrica, la cifra con su clave privada, y el resultado lo vuelve a cifrar con la clave pública de la otra parte (B), siendo el resultado de todo ello lo que se envía. Si entre A y B no hay ninguna relación previa al establecimiento de esa conexión segura, ¿qué problema presenta el protocolo descrito?

Ej.6. SSL/TLS es ampliamente usado en aplicaciones de comercio electrónico a través de web. Consulta en la bibliografía los pasos que se dan en SSL/TLS para establecer un canal seguro entre dos partes. Normalmente se usa la versión del protocolo que asume que el iniciador de la comunicación (el navegador), no va a presentar ningún certificado al servidor de la tienda virtual. ¿Cómo afecta esto a la seguridad de la comunicación entre navegador y servidor? Analícese por separado cada una de las tres características de la comunicación segura (confidencialidad, integridad, autenticación).

Ej.7. Utilizando técnicas de criptografía asimétrica, se puede garantizar la confidencialidad de un mensaje M cifrando el mensaje con la clave pública del receptor (sea B ese receptor). Por otra parte, se puede garantizar la autenticación del emisor del mensaje (sea A ese emisor) cifrándolo con la clave privada de A. Basándose en todo ello, nos proponen el siguiente esquema de cifrado en una comunicación, con objeto de garantizar la confidencialidad y autenticación en la misma:



Responde a las siguientes preguntas:

a) ¿Le ves algún inconveniente a este sistema? Supón que no hay ninguna duda respecto a la validez de las claves públicas.
b) Si le ves algún problema ¿cómo lo solucionarías?
c) Completa la propuesta para garantizar también la integridad y el no repudio del mensaje.

Ej.8. Se va a diseñar una aplicación cliente/servidor que dé el siguiente servicio:

- Los usuarios solicitan a través de Internet al servidor de la aplicación la generación de un certificado digital.
- Para ello, el servidor solicitará al usuario sus datos personales a consignar en el certificado.
- Recogidos esos datos, el servidor genera un par de claves pública/privada para el usuario, genera y firma el certificado, lo guarda en su base de datos, y envía, de manera cifrada, el par {certificado, clave privada} al usuario.

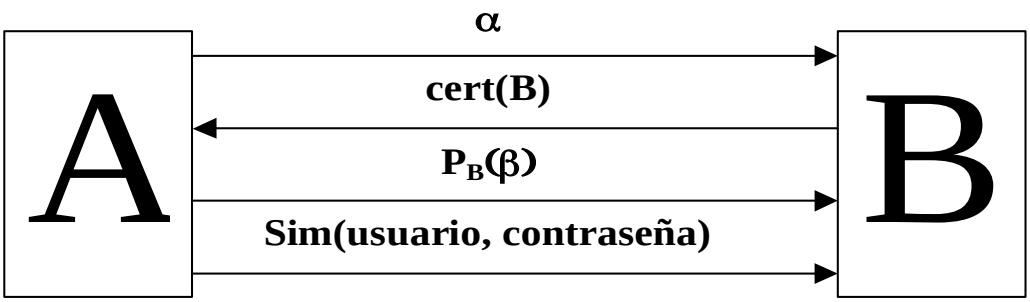
Se han establecido las siguientes condiciones al diseño y desarrollo de la aplicación:

- Será una aplicación web, en la que la recogida de datos se hará mediante un formulario. Rellenado y enviado el formulario, el usuario recibe como respuesta el par {certificado, clave privada}.
- La confidencialidad de la comunicación estará garantizada por el uso de SSL entre el servidor web y el navegador.
- El servidor web presentará su certificado al cliente para poder establecer la sesión SSL. Al usuario no se le solicita la presentación de ningún certificado.

Se pide:

Explica por qué un certificado emitido así no debería ser admitido como base para establecer una comunicación segura, sea quien sea el que firma el certificado.

Ej.9. Sea una aplicación en la que se ha definido un procedimiento para el establecimiento de una sesión segura entre un cliente A y un servidor B. Este procedimiento se basa en establecer primero una clave simétrica que garantice la confidencialidad, para después enviar un nombre de usuario y contraseña que autentique al cliente. Dicho procedimiento es el de la figura:



1) A envía a B un número aleatorio α.
2) B le devuelve su certificado.
3) A entrega ahora un nuevo número aleatorio ß, cifrado esta vez con la clave pública de B.
4) Tanto A como B calculan la clave simétrica en función de los números α y ß.
5) A envía su identificador de usuario y contraseña, cifrados con la clave simétrica de sesión.

Se pide:

a) Demostrar que este protocolo es sensible a ataques por repetición.
b) Cambiar el protocolo para hacerlo invulnerable a un ataque de repetición.

Ej.10. Supongamos que tu pareja se ha ido a Australia para un año y que te comunicas con él/ella mediante correo electrónico ya que por teléfono sale muy caro. Para mantener la confidencialidad empleáis un sistema de correo electrónico seguro (con confidencialidad y firma basados en cifrado asimétrico), pero otra persona que se quiere hacer con los favores de tu media naranja ha

conseguido su clave privada. Su intención es suplantar tu personalidad y enviarle mensajes liantes en tu nombre hasta conseguir que se enfade contigo para que te deje.

a) ¿Lo logrará?

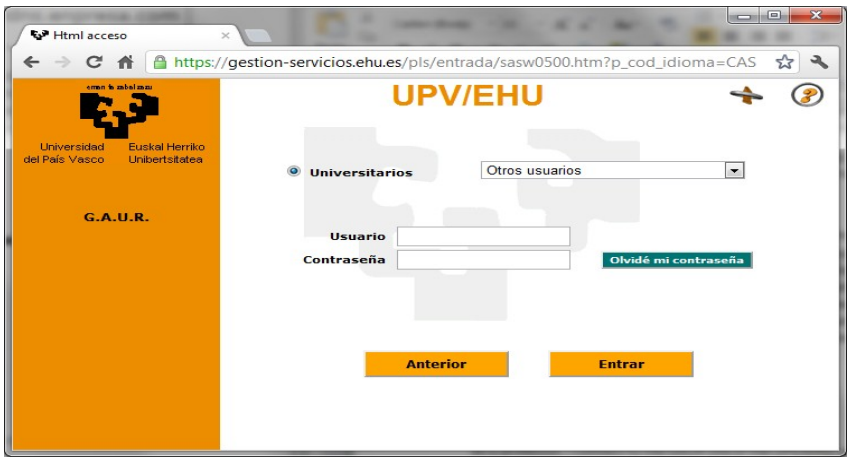
b) Si el oyente anterior intercepta un mensaje enviado por ti (puede hacerlo al disponer de la clave privada del receptor) y cambia su contenido, ¿cómo detectaría la argucia tu pareja?

c) Supongamos que has hecho correctamente el ejercicio anterior y que os habéis dado cuenta de que algo raro está pasando. Entonces, propones a tu pareja el cambio de todas las claves para andar más tranquilos, y establecéis el envío por correo convencional de las nuevas claves públicas pues ya receláis del correo. Tu contrincante intercepta tu propuesta, y, presa de la desesperación, no duda en sobornar al cartero de tu barrio, un hombre sin principios agobiado por las deudas de juego, para suplantar tu clave y las de tu pareja por otras entregadas por tu contrincante.

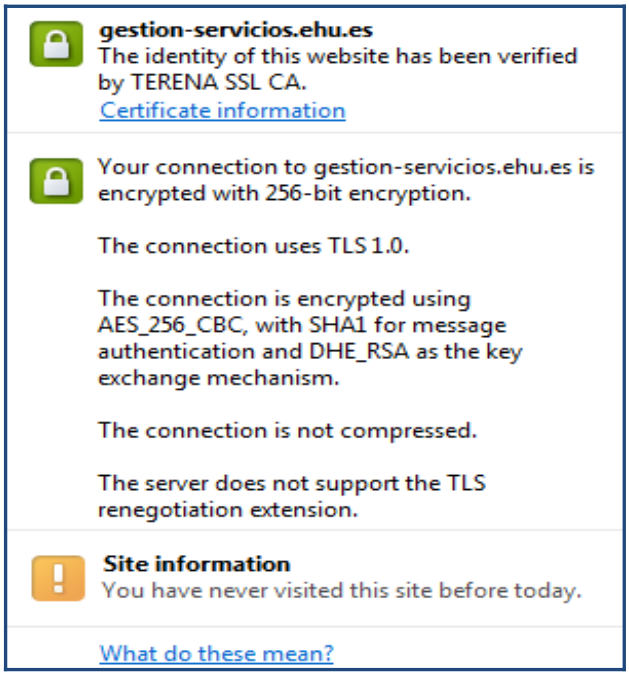
- Describe la situación que se creará a partir de ese momento ¿Qué mensajes, legibles e ilegibles, recibiréis los dos enamorados?
- ¿Era necesario prescindir del correo electrónico para intercambiar las nuevas claves? ¿Por qué?

d) Supongamos que el cartero, incómodo por los manejos de que es cómplice y atormentado por su conciencia, revelara al espía vuestras nuevas claves públicas a cambio del soborno, pero no las sustituyera por las falsas que éste le entrega. ¿En qué cambiaría esto la situación anterior?

Ej.11. Como profesor, al conectarme al portal GAUR de la UPV/EHU, observo la siguiente pantalla:



Haciendo clic en la zona verde puedo acceder a información adicional:



En base a dicha información, responde a las siguientes preguntas:

a) ¿Es la comunicación con el sitio GAUR confidencial? Si la respuesta es afirmativa, ¿Qué algoritmo se utiliza para garantizar la confidencialidad? ¿Qué tipo de algoritmo es?
b) ¿Puedo estar seguro acerca de la autenticidad del sitio GAUR? ¿Por qué?
c) Si la interacción con GAUR continua (tecleo usuario y password), puede estar seguro el sitio GAUR acerca de la autenticidad del usuario? ¿Por qué?
d) ¿Hay riesgo de que alguien ajeno obtenga el password tecleado?
e) ¿Pueden estar ambas partes seguras de la integridad de los mensajes intercambiados? ¿Por qué?
f) En base a las respuestas anteriores, ¿Qué sucedería si no tuviese en mi navegador el certificado TERENA SSL CA?
g) Indica como debería cambiar la interacción con GAUR en caso de querer utilizar una smart-card (dni-e, tarjeta universitaria) para acceder al servicio.

Ej.12. Estamos diseñando un protocolo de aplicación que garantice comunicaciones seguras. Para ello, antes de comenzar el intercambio de datos entre los usuarios A y B, será necesario establecer una conexión segura. Nos basaremos en certificados digitales, y el procedimiento será el siguiente:

a) A envía a B su certificado CERT_A
b) B crea una clave de sesión K_S para el cifrado simétrico de los datos
c) B envía K_S a A, utilizando Pub_A(K_S)

Una vez que ambos (A y B) conocen K_S, todos los mensajes intercambiados serán cifrados con dicha clave. Analiza en detalle si este protocolo cumple los requerimientos de una comunicación segura (¡como primer paso has de identificar dichos requerimientos!)

Ej.13. Las empresas A y B quieren realizar un intercambio seguro de documentos importantes a través de Internet. Acuerdan para ello utilizar en sus comunicaciones tanto criptografía simétrica como asimétrica (clave pública). La criptografía de clave pública será utilizada para firmar mensajes y para la autenticación inicial. La criptografía simétrica se utilizará para los intercambios de mensajes (clave de sesión).
Como no quieren realizar los procedimientos administrativos necesarios para solicitar certificados digitales a IZENPE (o cualquier otra autoridad de certificación) han decidido intercambiar (y

comprobar) sus claves públicas en persona (sin utilizar Internet). Suponiendo que posteriormente todos los intercambios de documentos entre ambas empresas se realizarán a través de correo electrónico,

a) Indica el procedimiento que puede utilizar A para enviar un mensaje “m” a B, garantizando confidencialidad. Indica el procedimiento ejecutado por B para recibir “m”.
b) Indica el procedimiento que puede utilizar A para enviar un mensaje firmado “m” a B. Indica el procedimiento ejecutado por B para verificar la identidad del emisor de “m”.
c) Indica si un mensaje firmado es o no confidencial. Indica, si es necesario, el procedimiento para enviar un mensaje “m” confidencial y firmado de A a B, así como los pasos que debe dar B para realizar las verificaciones necesarias.
d) Explica si existe un riesgo razonable de que T, una tercera compañía, suplante la identidad de A, al enviar mensajes firmados a B.
e) Indica los problemas que pueden aparecer al ampliar este esquema a otras empresas colaboradoras.

Ej.14. Sea un servicio para descargas mediante pago, que funciona así:

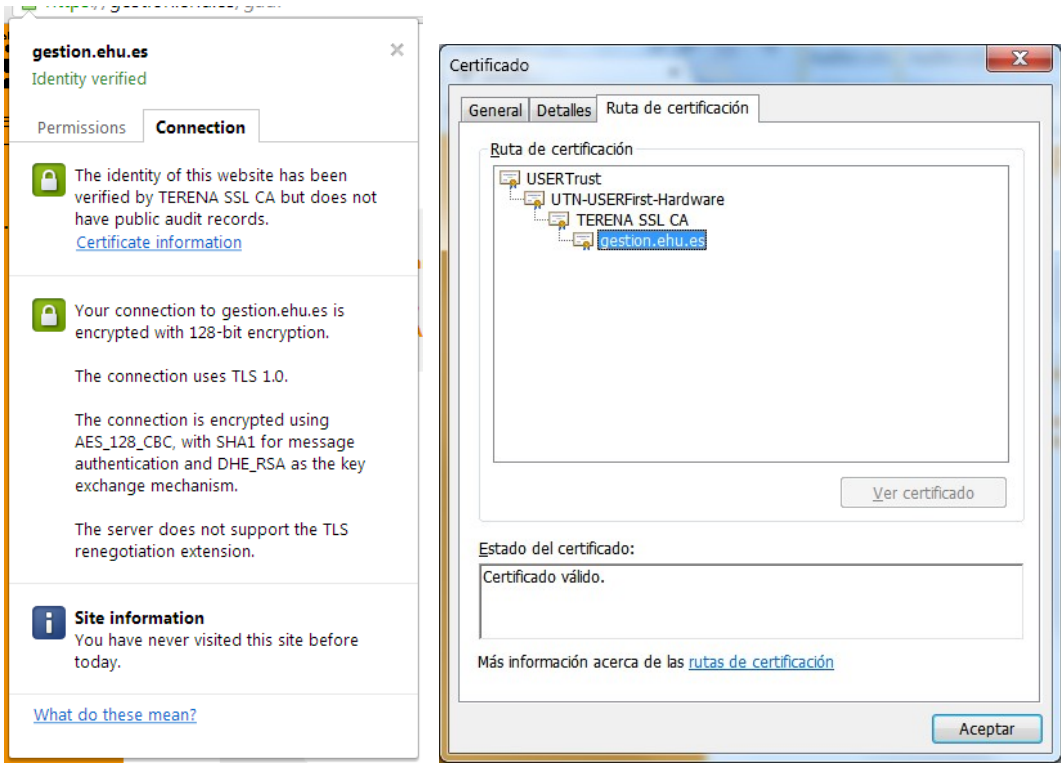
1. El comprador inicia una conexión SSL/TLS con la web del vendedor. Únicamente se exige al servidor disponer de certificado.
2. A través de esa conexión el comprador hace su petición de descarga y proporciona sus datos para facturación (identificación y dirección).
3. Se hace la descarga.
4. El vendedor envía al comprador la factura, usando los datos anteriores, por medios convencionales fuera de internet.

Un día, un comprador devuelve la factura al vendedor, alegando que el nunca ha hecho esa descarga. Van juicio, y te nombran perito. Como prueba, el vendedor presenta los logs de su maquina, donde esta registrada toda la operación según lo descrito antes. Puedes verificar que los logs son auténticos, y en ellos aparecen todos los mensajes de la descarga, con la identificación del demandado. En el juicio te plantean dos preguntas:

a) Abogado del vendedor: Analizados los datos, ¿Puede darse por probado que el demandado solicitó e hizo la descarga, pese a que ahora lo niegue para no hacerse cargo del pago correspondiente?
b) Abogado del supuesto comprador demandado: ¿Es posible que, aunque los logs registrados en el servidor sean auténticos y por tanto se haya producido esa descarga, el vendedor haya sido quien ha simulado esa venta, para ahora reclamar la factura al acusado?

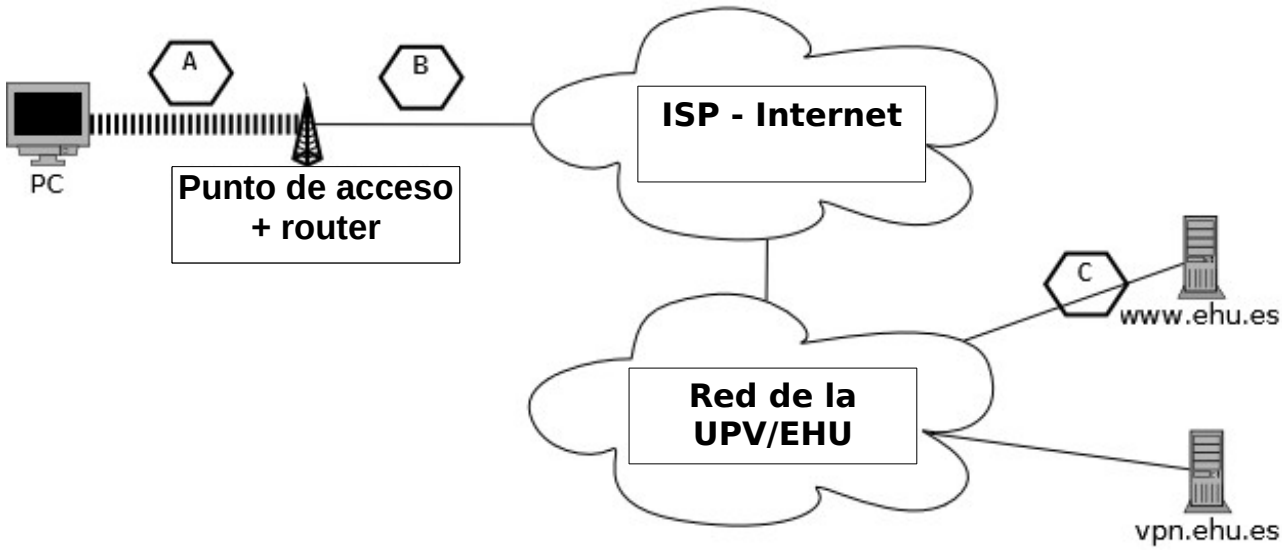
Expón tus respuestas.

Ej.15. Al conectarme a través de un navegador a la web de GAUR, puedo observar que estoy utilizando una conexión “segura”. Puedo obtener información adicional, como la que se muestra en la figura (lado izquierdo). Adicionalmente, al hacer click en “Certificate information”, se muestra la siguiente información (lado derecho de la figura)



a) Explica que es (para que se utilizan) los siguientes elementos:
   1. AES_128_CBC
   2. SHA1
   3. DHE_RSA
b) Explica el significado de “The certificate is OK” (certificado válido), y “Certification Path” (Ruta de certificación) en el lado derecho de la figura.
c) Explica si te puedes fiar o no del servidor de la UPV/EHU que alberga GAUR (gestion.ehu.es), y si la UPV/EHU se puede fiar de ti como usuario autorizado de GAUR.

Ej.16. La UPV/EHU ofrece un servicio de Red Privada Virtual (VPN) para poder acceder a los servicios de la universidad cuando se está fuera de la misma. En vuestro hogar disponéis de una conexión ADSL (punto de acceso + router) contratada con un proveedor ISP. Vuestro PC se conecta con vuestro punto de acceso+router por vía inalámbrica (utiliza además WPA2). La dirección IP (proporcionada por el ISP) es 171.2.2.2/30. Tu dirección IP UPV/EHU (proporcionada por el servidor VPN) es 158.227.240.123/16, y la dirección IP del servidor VPN de la UPV/EHU (vpn.ehu.es, 158.227.1.3).



Supón que, una vez creado el túnel VPN, estableces una comunicación con el servidor web de la UPV/EHU (www.ehu.es, 158.227.20.1) usando HTTP. Teniendo en cuenta que hay instalados 3 sniffers en los puntos A, B, y C, indica si será posible obtener la siguiente información (y en caso afirmativo indica los valores observados) en cada uno de los puntos mencionados:

- Direcciones IP de origen y destino
- Puertos de origen y destino
- Datos (petición HTTP realizada)

Ej.17. Has montado una empresa para ofrecer un servicio de traducción de documentos del castellano al inglés. Los clientes te envían sus documentos a través de la red y tú les envías el primer párrafo del documento traducido sin ningún coste (párrafo de muestra). Si el cliente está satisfecho deberá enviarte sus datos de facturación y tú le responderás, en un plazo razonable, con el documento traducido.
Para realizar todo el proceso con seguridad has diseñado el siguiente sistema:

1. El cliente te envía el documento a traducir. No consideras que esta parte requiera ninguna medida de seguridad por lo que el documento va sin cifrar.
2. Le respondes con el párrafo de muestra. Este párrafo no lo consideras confidencial por lo que no lo cifras, pero como no quieres que nadie lo pueda cambiar, adjuntas el resumen Hash del párrafo para obtener integridad. De esta manera, si alguien lo cambia, el resumen Hash dejará de ser válido.
3. Si el cliente está satisfecho te envía sus datos de facturación firmados con su DNI electrónico. Para que puedas validar la firma, te adjunta el certificado digital de su DNI electrónico emitido por la Dirección General de la Policía (DGP). Dado que el certificado incluye su nombre y número de DNI, el cliente queda autenticado.
4. Envías al cliente el documento traducido. Dado que quieres que este documento sea confidencial y autenticado, lo cifras con una clave simétrica de sesión y cifras la clave

simétrica con la clave pública del cliente. Así, además de seguridad, consigues eficiencia. Envías al cliente los dos criptogramas: el documento cifrado con clave simétrica y la clave simétrica cifrada con la clave pública del cliente.

Responde a las siguientes preguntas:

a) Imagina que otra empresa de la competencia quiere quitarte los clientes. Para ello, intercepta el párrafo de muestra que envías en el paso 2 y lo modifica introduciendo errores de traducción. ¿Es posible que lo haga sin que el cliente se dé cuenta de ello? Si es que sí, explica cómo y si es que no, explica por qué.

b) Cuando en el paso 3 recibes el certificado del cliente, ¿qué necesitas para validar el certificado? Y ¿qué elemento del certificado necesitas para validar la firma del cliente? No indiques cómo es el proceso, sino los elementos que necesitas para cada operación.

c) En el paso 4, ¿el traductor (es decir, tú) está autenticado? Si es que sí, explica por qué y si es que no, indica una forma de añadir la autenticación del traductor.

Ej. 18. Supongamos que el emisor A envía un mensaje M siguiendo el siguiente esquema:

$$[Priv_A(M), \text{Identificación\_A}]$$

Es decir, el mensaje se cifra con la clave privada del emisor, y se envía junto a la identificación del emisor A.

- ¿Se garantiza la confidencialidad de la comunicación?
- ¿Qué ventajas tendría el uso de la firma digital en lugar del esquema propuesto?

Ej. 19. Conectado a un sitio web, puede verse un candado en la ventana del navegador. Cliquando en el candado (‘más información’) aparece la ventana de la figura (a). En esa ventana, al cliquar en “Ver certificado” aparece otra ventana como la de la figura (b). Finalmente, en la configuración de tu navegador, en la opción de ‘Seguridad’, cliquas en el botón “ver certificados” y puedes ver las ventanas de las figuras (c) y (d).

Realiza un análisis de seguridad de la conexión, teniendo en cuenta todas las caracteristicas de seguridad. Razona cada afirmación en base a la información que aparece en las figuras.

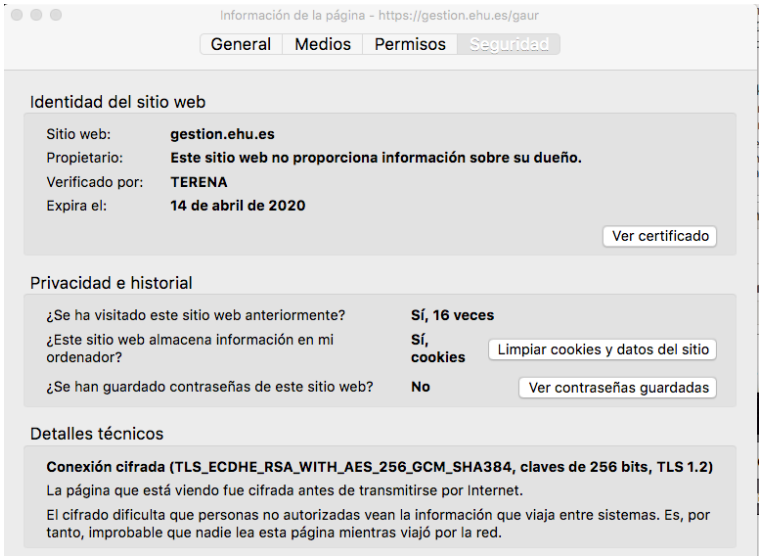


Figura (a)

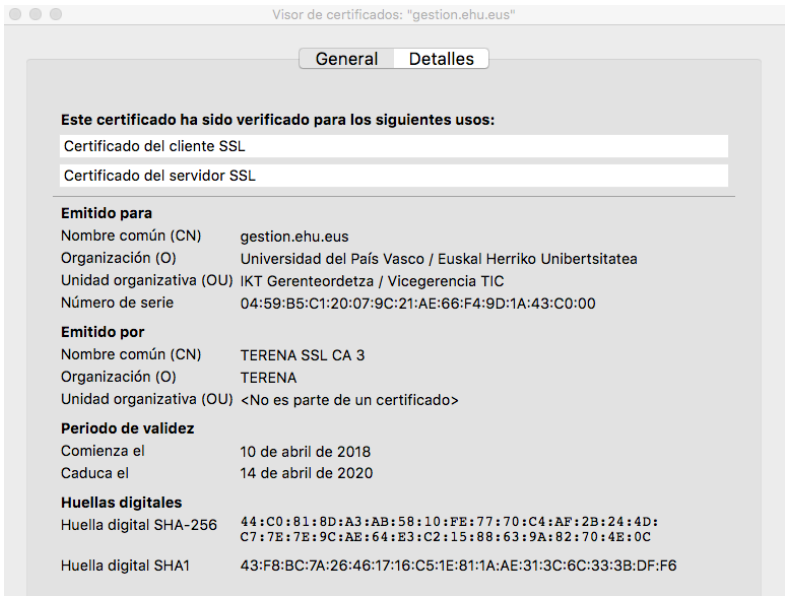


Figura (b)

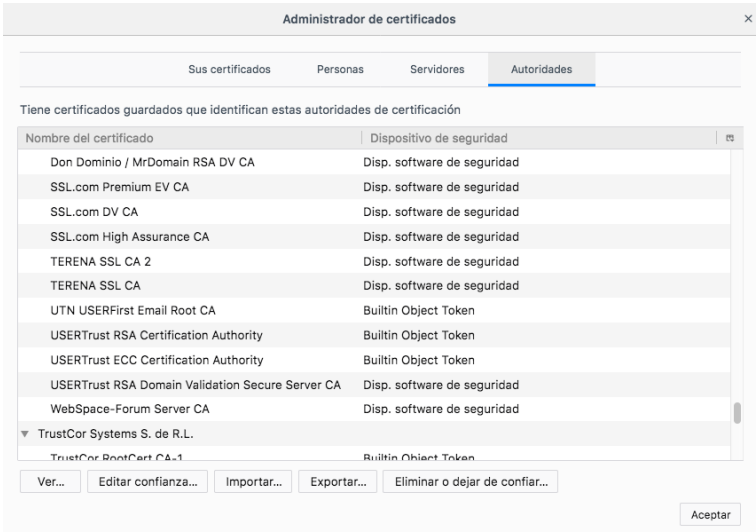


Figura (c)

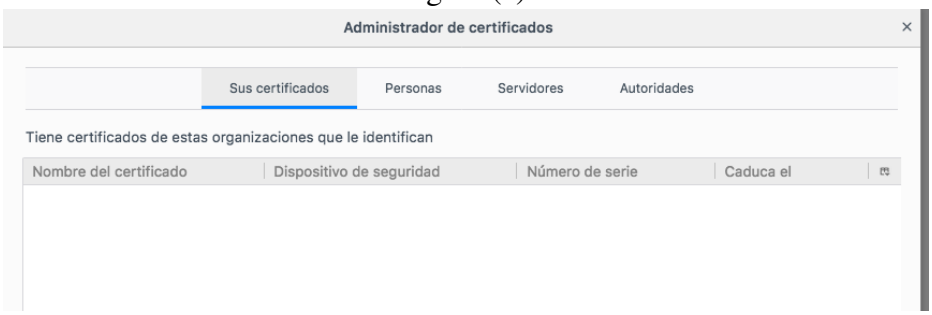


Figura (d)

Ej. 20. Utilizamos un sistema para enviar mensajes confidenciales y firmados utilizando una combinación de funciones hash, criptografía simétrica y criptografía de clave pública (asimétrica). Nuestro sistema no utiliza certificados. Cada usuario genera su par de claves y para tener confianza en la legitimidad de las claves públicas del resto de usuarios es necesaria una reunión presencial. Por ejemplo, en la reunión presencial entre Alice y Bob, Bob entrega a Alice una tarjeta de papel en la que hay escritos sus datos personales (nombre, n.º DNI, domicilio…) y el resumen hash de su clave pública, es decir, H(PubB). Alice tiene la posibilidad de comprobar que los datos personales de la tarjeta de Bob son correctos por lo que puede asegurarse de que nadie se está haciendo pasar por él. En esa misma reunión Alice puede dar una tarjeta equivalente a Bob y este puede verificar su identidad de la misma manera.
El sistema se completa con un repositorio público donde se almacenan las claves públicas de todos los usuarios. Su acceso es público y cualquiera puede subir una clave pública asociada a una identidad. Por eso, son necesarias las reuniones y el intercambio de tarjetas para dar legitimidad a las claves públicas obtenidas desde el repositorio.
Es decir, podrás obtener cualquier clave pública desde el repositorio, pero solo podrás verificar la validez de aquellas claves con cuyos usuarios te has reunido. En cuanto a los usuarios con los que no te has reunido y, por tanto, aún no tienes su tarjeta, podrás obtener su clave pública desde el repositorio, pero no podrás fiarte de ella.
Para realizar los siguientes ejercicios asume que Alice y Bob se han reunido y han intercambiado sus claves tal y como se ha indicado anteriormente. Trudy, en cambio, no se ha reunido con nadie. Las claves públicas de estos tres usuarios están en el repositorio de claves y asume que todo lo que debe ser secreto es secreto. Es decir, nadie conoce ninguna clave que no debería conocer.

a) Alice obtiene la clave pública de Bob desde el repositorio. Explica cómo utiliza Alice la información que le da Bob en la tarjeta de la reunión presencial para verificar la legitimidad de la clave obtenida.

b) Bob envía un mensaje confidencial a Alice. Para hacerlo de forma eficiente utiliza una clave de sesión simétrica para cifrar el mensaje y criptografía de clave pública (asimétrica) para compartir la clave de sesión. Explica cómo lo hará usando la notación abreviada usada habitualmente en clase. Recuerda que solo necesita que el mensaje sea confidencial.
c) Trudy envía un mensaje a Alice usando el mismo sistema que en el apartado anterior. Índica la estructura del mensaje. ¿Será el mensaje realmente confidencial en este caso?
d) Bob envía un mensaje firmado a Alice. Escribe la estructura del mensaje. Recuerda que debe ser eficiente y que no es necesario que el mensaje sea confidencial. ¿Puede Alice verificar que el mensaje es realmente de Bob? Si es que sí, explica cómo lo hará. Si es que no, explica por qué.
e) Trudy, usando sus claves, envía un mensaje firmado a Alice, pero intenta hacerse pasar por Bob. Escribe la estructura del mensaje. ¿Qué ocurrirá cuando Alice verifique la firma para comprobar si realmente lo envía Bob?
f) Trudy envía un mensaje firmado a Alice usando su propia identidad (no intenta hacerse pasar por nadie). Escribe la estructura del mensaje. ¿Puede Alice confiar en que el mensaje es realmente de Trudy?

Ej. 21. Estás desarrollando un sistema para aportar seguridad a las comunicaciones dentro de una entidad. Para ello, has instalado un servidor de claves simétricas, llamado S. Para obtener una clave simétrica compartida entre A y B (K_{AB}), se ha definido un protocolo de tres envíos que funciona de la siguiente manera:

(1) Para que A y B puedan usar S, previamente han tenido que hacer llegar a S sus respectivas claves públicas PubA y PubB. Para ello, el protocolo define un procedimiento de registro consistente en enviar a S un certificado firmado por alguna autoridad reconocida por el sistema.

(2) Cuando A quiere comunicarse de forma segura con B, lanza una petición al servidor de claves S, solicitándole una clave simétrica de sesión K_{AB}:

$A \rightarrow S$: (Soy A, quiero hablar con B)

(3) El servidor S genera la clave solicitada K_{AB}, y genera una respuesta a A que contiene dos copias protegidas de la clave generada, una para A (cifrada con la clave pública de A) y otra para B (cifrada con la clave pública de B).

$S \rightarrow A$: (PubA(K_{AB}), PubB(K_{AB}))

(4) A envía su petición de conexión a B, acompañada de la copia protegida de K_{AB} que le ha entregado el servidor S para que la reenvíe a B. En este momento tanto A como B compartirán K_{AB}.

$A \rightarrow B$: (Soy A, PubB(K_{AB}))

a) ¿Está garantizada la confidencialidad de la clave simétrica K_{AB}? En caso afirmativo explícalo, en caso negativo ofrece un contraejemplo.
b) Explica cómo un atacante T podría establecer una sesión con B haciéndole creer que es A.

Para evitar suplantaciones de identidad, el protocolo se reformula de la siguiente forma:

(1) Previamente, A y B se registran en S enviándole sus certificados. Además, ahora se descargan el certificado de S.

(2) Cuando A quiere comunicarse de forma segura con B, lanza una petición al servidor de claves S, solicitándole una clave simétrica de sesión K_{AB}. Además, ahora esa solicitud irá firmada:

$A \rightarrow S$: (Soy A, quiero hablar con B) + firmaA(solicitud).

(3) El servidor S genera la clave solicitada K_{AB}, y genera una respuesta a A que contiene dos copias protegidas de la clave generada, una para A (cifrada con la clave pública de A) y otra para B (cifrada con la clave pública de B). Además, ahora el servidor añadirá la identidad de A firmada.

$S \rightarrow A$: (PubA(K_{AB}), PubB(K_{AB})) + firmaS(Sí, es A).

(4) A envía su petición de conexión a B, acompañada de la copia protegida de K_{AB} que le ha entregado el servidor S para que la reenvíe a B. En este momento tanto A como B compartirán K_{AB}. Además, ahora A envía a B su identidad firmada por el servidor S.

A → B: (Soy A, PubB(K_{AB})) + firmaS(Sí, es A).

c) Explica cómo un atacante T podría seguir estableciendo una sesión con B haciéndole creer que es A. Ten en cuenta para ello que el atacante T puede intervenir las comunicaciones en la red.
d) Modifica el protocolo de alguna forma para que T no pueda suplantar a A. Hazlo sin que A y B tengan que intercambiar certificados entre ellos.

Ej. 22. Estoy desarrollando una plataforma de videojuegos en la que quiero que todas las comunicaciones entre jugadores tengan garantías de confidencialidad, autenticación e integridad. Para ello, inspirado en TLS, implemento el siguiente protocolo:

1. El servidor de la plataforma funciona como una autoridad de certificación. El proceso para emitir un certificado es el siguiente:
   a) El jugador, J, inicia una comunicación segura con el servidor usando TLS.
   b) J inicia sesión en el servidor con su usuario y contraseña.
   c) J genera una par de claves asimétricas en su ordenador, PrivJ y PubJ, y envía PubJ al servidor.
   d) El servidor envía un reto al jugador para que demuestre que dispone de la clave PrivJ.
   e) El servidor genera un certificado para el jugador, CertJ, y se la envía a J o a cualquier otro jugador que lo solicite.
   f) El servidor envía su certificado, CertS, a J.
2. Cuando dos jugadores, J1 y J2, quieren jugar, pueden intercambiarse información siguiente el siguiente proceso a través de una conexión TCP:
   a) J1 y J2 intercambian sus certificados y verifican su validez.
   b) J1 envía un reto, R1, a J2 para que demuestre que tiene la clave privada correspondientes a la clave pública disponible en su certificado. J2 hace lo mismo con J1, enviándole otro reto, R2. Ambos responden con la demostración.
   c) J1 y J2 utilizan Diffie-Hellman para establecer una clave simétrica de sesión, Ks.
   d) J1 y J2 calculan una segunda clave simétrica, Km, a partir de Ks (esto se puede realizar de forma segura).
   e) Los datos intercambiados entre J1 y J2 se dividen en bloques a los que se añade un número de secuencia. Para cada bloque se calcula su MAC (Message Authentication Code) usando Km y se cifra el bloque usando Ks.
   f) J1 y J2 se intercambian los bloques cifrados, adjuntando su correspondiente MAC.

- Explica un modo alternativo para generar las claves asimétricas si los jugadores no tienen capacidad para generarlas por ellos mismos. Explica las ventajas y/o desventajas de esta alternativa.
- Explica los pasos necesarios para realizar los pasos 2a y 2b. Explica por qué estos pasos autentican a los jugadores.
- Explica qué pasos sigue el receptor de un bloque en el paso 2e y por qué este paso provee confidencialidad e integridad.

Ej. AUTOEVALUACIÓN. Establecer la correspondencia entre los siguientes acrónimos y términos con su definición.

Firma digital		TLS / SSL		Criptografía simétrica	
Criptografía		WEP		Confidencialidad	
Red perimetral o DMZ		Diffie-Hellman		Servidor de claves	
IPsec		Integridad		X.509	
Intranet		VPN		Autenticación	
Certificado digital		No repudio		Criptografía asimétrica	
Cortafuegos		Extranet		WPA3	

(1) Red local con servidores especialmente protegidos contra ataques.
(2) Máquina que filtra el tráfico entre dos redes.
(3) Red TCP / IP que tiene el acceso cerrado a los usuarios externos.
(4) Parte de una red interna que está abierta de forma controlada a usuarios fuera de ella
(5) Característica de la comunicación que garantiza que la información intercambida solo es conocida por el emisor y el receptor.
(6) En una comunicación, garantiza la identidad de la otra parte.
(7) Característica de la comunicación que garantiza que la información intercambiada entre el emisor y el receptor no ha cambiado.
(8) Característica de la comunicación que garantiza que el emisor no puede negar que ha envidado el mensaje.
(9) Análisis y uso de técnicas de cifrado para garantizar la confidencialidad de la información.
(10) Criptografía que utiliza la misma clave de cifrado y descifrado.
(11) Criptografía que utiliza diferentes claves de cifrado y descifrado.

(12) Servidor que genera y distribuye claves para una sesión de comunicación.
(13) Algoritmo para establecer una clave simétrica, usando canales de transmisión públicos, que garantiza la confidencialidad de la clave.
(14) Técnica que garantiza la integridad y no repudio de un mensaje.
(15) Documento firmado digitalmente por alguien de confianza que asocia una identidad a una clave pública.
(16) Formato estándar de certificados digitales para la distribución de claves públicas.
(17) Protocolo para establecer sesiones seguras basadas en certificados.

(18) Técnica que garantiza la seguridad de las comunicaciones entre subredes de una red privada a través de Internet, basada en túneles encriptados.
(19) Estándar para garantizar la seguridad de los datagramas IP.
(20) Estándar no seguro para la comunicaciones en redes Wi-Fi.
(21) Estándar seguro para la comunicaciones en redes Wi-Fi.