Estudios de Informática, Multimedia y Telecomunicación

Redes y Aplicaciones Internet

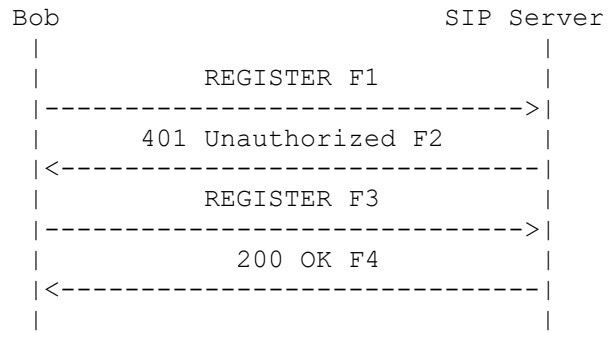
Reto 6

PEC 3 – Tercera Prueba de Evaluación Continua

- Hay que entregar la solución en un fichero preferiblemente pdf, utilizando la plantilla adecuada, en el registro de evaluación continua.
- La fecha límite de entrega es el 15 de mayo de 2022

Respuestas

1. Dado el siguiente intercambio de comandos SIP, incluyendo sus peticiones y respuestas:



F1

```
REGISTER sips:ss2.biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashds7
Max-Forwards: 70
From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl
To: Bob <sips:bob@biloxi.example.com>
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 1 REGISTER
Contact: <sips:bob@client.biloxi.example.com>
Content-Length: 0
```

F2

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashds7
 ;received=192.0.2.201
From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl
To: Bob <sips:bob@biloxi.example.com>;tag=1410948204
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 1 REGISTER
```

```
WWW-Authenticate: Digest realm="atlanta.example.com", qop="auth",
 nonce="ea9c8e88df84f1cec4341ae6cbe5a359",
 opaque="", stale=FALSE, algorithm=MD5
Content-Length: 0

F3

REGISTER sips:ss2.biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashd92
Max-Forwards: 70
From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH
To: Bob <sips:bob@biloxi.example.com>
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 2 REGISTER
Contact: <sips:bob@client.biloxi.example.com>
Authorization: Digest username="bob", realm="atlanta.example.com"
 nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",
 uri="sips:ss2.biloxi.example.com",
 response="dfe56131d1958046689d83306477ecc"
Content-Length: 0

F4

SIP/2.0 200 OK
Via: SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashd92
 ;received=192.0.2.201
From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH
To: Bob <sips:bob@biloxi.example.com>;tag=37GkEhwl6
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 2 REGISTER
Contact: <sips:bob@client.biloxi.example.com>;expires=3600
Content-Length: 0
```

a) Describe brevemente qué es lo que ha pasado en este intercambio de mensajes SIP. ¿Cuántas máquinas hay involucradas? Razona tu respuesta.

b) Este intercambio de mensajes, ¿se ha hecho de manera segura? Razona tu respuesta.

c) Describe el significado de las cabeceras From, To y Cseq que aparecen en los siguientes mensajes y di si existe alguna relación entre ellas.

d) ¿Qué diferencia hay entre los mensajes SIP F1 y F3? ¿Y entre F2 y F4? ¿A qué crees que se deben estas diferencias? Razona tu respuesta.

a) Bob hace una petición de registro en su servidor, pero este retorna un error 401 y le pide autenticación (F2). Bob vuelve a enviar la petición de registro con los datos requeridos (cabecera Authorization en F3) y entonces el servidor lo acepta (F4). Hay dos máquinas, la de Bob y el SIP server.

b) Sí, porque se utiliza la versión segura del protocolo, sips, y, además, se indica en las cabeceras que se utiliza TLS.

c) From indica quien hace la petición. To indica quien recibe la petición. Cseq indica el número de la secuencia del comando. El valor de Cseq se repite en la petición y la respuesta.

d)

```
Authorization: Digest username="bob", realm="atlanta.example.com"
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",
uri="sips:ss2.biloxi.example.com",
response="dfe56131d1958046689d83306477ecc"
```

La diferencia entre F1 y F3 se debe a que el servidor necesita autenticación.

La diferencia entre F2 y F4 se debe a que Bob envía los datos requeridos al servidor.

2. El estándar MPEG-DASH define un mecanismo mediante el cual el cliente pide los contenidos en función de las condiciones de la red. Responde razonadamente a las siguientes cuestiones:
   a) ¿Dónde se define el contenido que el cliente puede descargar? ¿En qué formato está esta definición?
   b) ¿Cómo se organiza el contenido para que pueda ser descargado? ¿Por qué esto simplifica la implementación del servidor?
   c) ¿Qué técnica puede mejorar la descarga de los contenidos en el lado cliente?

   a) En un fichero MPD (Media Presentation Description). Este fichero utiliza el formato XML. En el libro se puede encontrar lo que es un manifest file.
   b) El contenido se divide en segmentos de diferentes calidades. En función de la conexión de red, se pueden pedir segmentos de mejor o peor calidad. Quien decide qué calidad de segmento pide es el cliente. El servidor sólo tiene que almacenar los segmentos y servirlos cuando el cliente los pida.
   c) El *buffering*. Si el cliente tiene mucho contenido en el *buffer*, podrá pedir contenidos de mejor calidad.

3. Real-time Transport Protocol (RTP) es un protocolo que se utiliza para hacer *streaming* de contenidos. Responde razonadamente a las siguientes cuestiones:
   a) ¿Se puede utilizar TLS (Transport Layer Security) con RTP?
   b) ¿Existe alguna empresa que utilice este protocolo para retransmitir sus contenidos? En caso afirmativo, busca información de cómo se hace la transmisión con RTP de contenidos multimedia.

   a) Sí, de esta forma se envían los datos RTP de forma segura. El protocolo SRTP (Secure RTP) se define en https://datatracker.ietf.org/doc/rfc3711/ y tiene dos revisiones, la RFC 5506 y la RFC 6904.
   b) Sí, Movistar o Vodafone utilizan RTP. Podéis encontrar las direcciones de los canales RTP de Movistar en: https://www.web-futbol.com/lista-actualizada-de-canales-para-vlc-2020/

4. En el libro se explica en detalle qué es el *jitter* y las técnicas que permiten reducirlo. Indica cuáles son y en qué consisten. Además, busca información de cuál es el *jitter* máximo aceptable para poder jugar de forma on-line de forma satisfactoria. Indica todas las fuentes de información que hayas consultado.

En la reproducción con retardo fijo, el receptor intenta reproducir cada paquete exactamente "q" milisegundos después de que se haya generado. Por eso, a cada paquete se le pone una marca de tiempo (*timestamp*) "t" cuando se genera y se reproduce en el instante "t+q". Si un paquete llega más tarde que "t+q" no se puede reproducir y se da por perdido.

En la reproducción con retardo variable el receptor no intenta reproducir cada paquete exactamente después de una cantidad de tiempo fija, sino que se reproduce en función de las condiciones de la red durante la sesión de audio. Es decir, "q" es variable y se van adaptando en relación con el retardo de la red y de la variación de este retardo.

El *jitter* adecuado para jugar tiene que estar por debajo de 60 ms. Los valores ideales están entre 20 y 40 ms y no sólo dependen de la conexión del usuario sino también de donde está el servidor.

https://www.redeszone.net/tutoriales/redes-cable/mejorar-latencia-jugar-online/

https://blogthinkbig.com/jitter-velocidad-conexion-internet

https://bandaancha.eu/articulos/cual-mejor-compania-fibra-jugar-online-9894

https://www.testdevelocidad.es/2017/08/18/cuanto-ping-injugable-juego-online/

5. Busca información de cómo se puede saber si tu *router* de casa o del trabajo tiene activados mecanismos de *Quality of Service* (QoS) y descríbelos brevemente. Indica todas las fuentes de información que hayas consultado.

   Respuesta libre que depende del modelo de router que tengáis. Si no lo sabéis, podéis responder de forma teórica con algún manual de router que encontréis en Internet.

   https://quantumpc.com/qos-router-setting/

   https://comunidad.movistar.es/t5/Soporte-Fibra-y-ADSL/QoS-que-es-y-c%C3%B3mo-activarlo/td-p/3620545

   https://www.testdevelocidad.es/configuraciones/que-es-el-qos-de-un-router-y-como-configurarlo/

6. Queremos hacer una encriptación polialfabética (*polyalphabetic encryption*) con 2 alfabetos, donde el primer alfabeto (C1) sea un cifrado César y el segundo (C2) sea un cifrado monoalfabético. Define los 2 alfabetos, diferentes de los del libro, fija el patrón de repetición (*repeating pattern*), que puede ser de cualquier número de elementos (no hace falta que sea de 5 cómo en el libro), y codifica un breve mensaje (10-20 caracteres) que incluya tu nombre (o apellido).

   - Nota: al igual que en el libro, utiliza sólo el alfabeto inglés, letras en minúsculas, y los espacios y signos de puntuación se mantienen iguales en el texto cifrado, y no cuentan (como si no estuvieran) al aplicar el patrón de repetición.

```
Plaintext     a b c d e f g h i j k l m n o p q r s t u v w x y z
Ctxt C1 (k=5) f g h i j k l m n o p q r s t u v w x y z a b c d e
Cyphtext C2   m n b v c x z a s d f g h j k l p o i u y t r e w q
```

```
Patrón de repetición: C2, C1, C1, C2, C1

Plaintext       bob, i love you.
Cyphertext      ntg, s qkaj wty.
```

7. Justifica si las siguientes afirmaciones son ciertas o no. En el supuesto de que haya más de una falsedad, justifícalas todas (o corrígelas todas):
   a) En un certificado la seguridad (confidencialidad e integridad) se proporciona cifrando todos los campos con la clave secreta de la Autoridad de Certificación.
   b) El mecanismo de Diffie-Hellman (que tiene cierto parecido con RSA) nos permite generar e intercambiar de forma segura una clave pública a través de un canal inseguro.
   c) Una clave de sesión es una clave normalmente simétrica para ser usada "1 sola vez/conexión" que nos proporciona autenticación de origen.
   d) Si podemos descifrar un mensaje utilizando la clave privada de Alice, es que aquel mensaje lo ha generado ella (y por lo tanto tenemos autenticación de origen).

   a) Falso. Proporciona autenticación de origen y no confidencialidad, y se cifra el hash de todos los campos (se firma).
   b) Falso. El mecanismo Diffie Hellman nos permite el intercambio de claves simétricas (a menudo claves de sesión) de forma segura a través de un canal inseguro. Las claves públicas son públicas y por tanto se pueden intercambiar sin cifrar solo añadiendo un mecanismo de autenticación e integridad (típicamente las claves públicas se intercambiarán junto con otros parámetros dentro de un certificado, que está firmado).
   c) Falso. El uso de claves simétricas es en principio más seguro y mucho menos costoso computacionalmente, pero no permite autenticación. Entonces lo que se hace a menudo (p.e. SSL/TLS) es al inicio de una sesión/conexión una autenticación de los usuarios con claves asimétricas y un posterior intercambio seguro de una clave simétrica (p.e. con el método Diffie Hellman) que es la que se utiliza para el intercambio de los datos.
   d) Falso. Tendría que ser con la pública. La privada solo la tiene ella.

8. La figura 8.21 del libro (página 657) es la combinación de las figuras 8.19 y 8.20 por lo que respecta al emisor del mensaje. Haz un diagrama que ilustre qué haría el receptor que estaría a la derecha de la figura 8.21, y explícalo brevemente.

   Bob recibirá el mensaje+hash, todo encriptado con una clave simétrica, y además esta clave, encriptada con la clave pública de Bob. Bob aplica su clave secreta para obtener la clave simétrica, y con ella obtiene el mensaje+hash desencriptando lo que ha recibido. Y con la clave pública de Alice genera el hash, y lo compara con el que ha recibido.

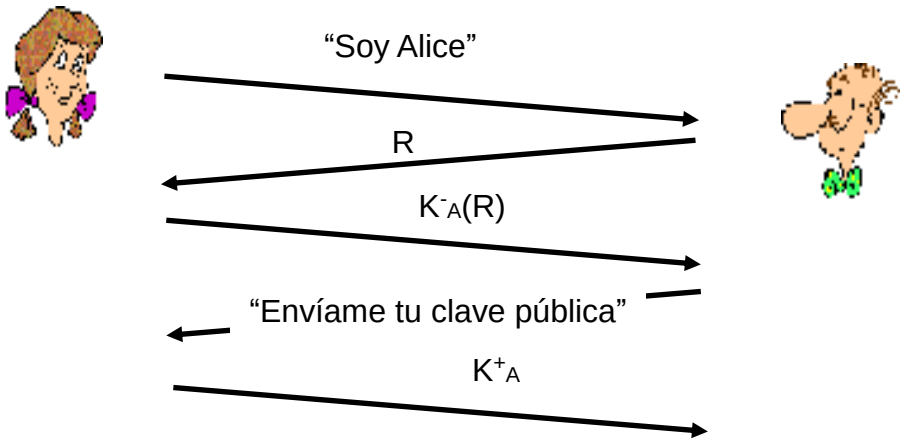
9. El protocolo de autenticación ap4.0 para proporcionar *endpoint authentication* usa un *nonce* y encriptación simétrica (explicado en la página 652 del libro). Si usamos encriptación de clave pública entonces tenemos el ap5.0. Considera el siguiente protocolo:

    1. Alice envía el mensaje “soy Alice” a Bob
    2. Bob escoge un *nonce* R y lo envía a Alice
    3. Alice encripta con su clave privada el *nonce* y envía el resultado a Bob
    4. Bob aplica la clave pública de Alice al mensaje recibido y obtiene R

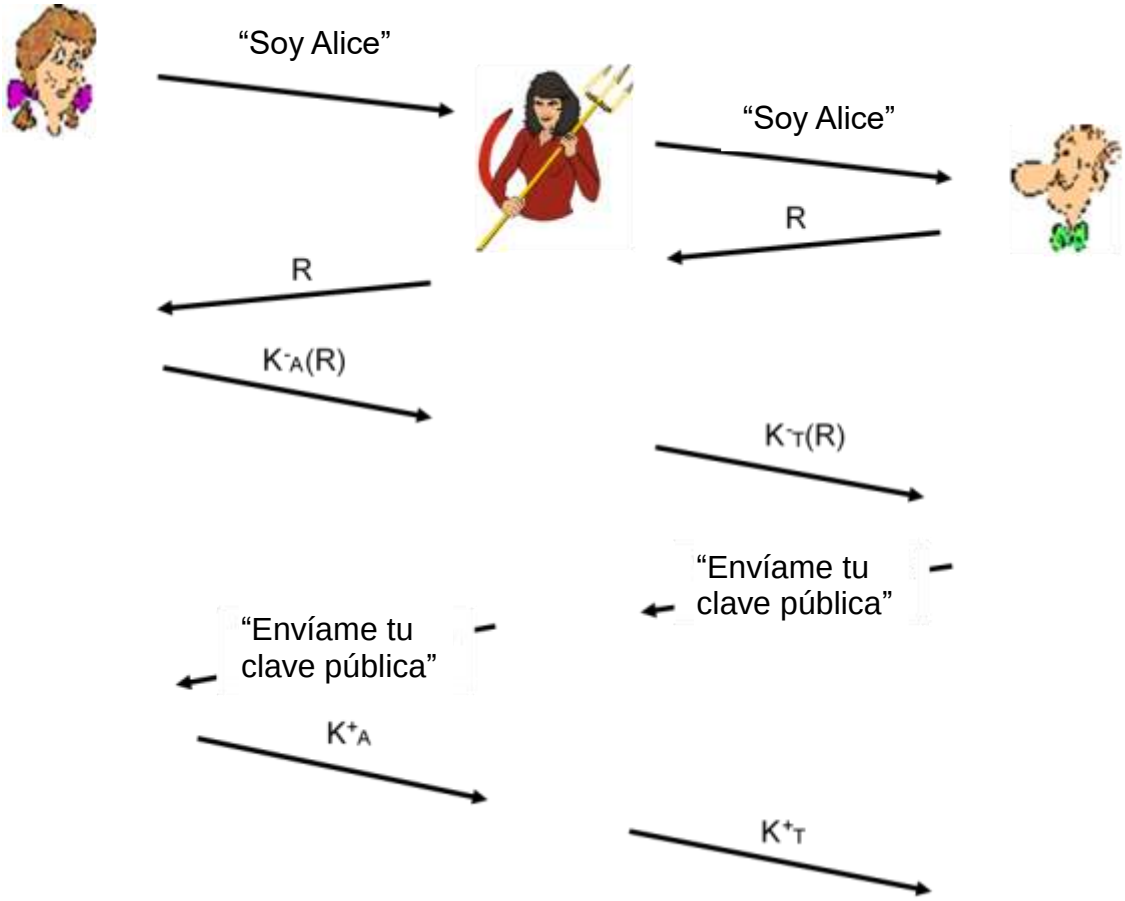
    a) Haz un diagrama del protocolo, usando la notación para las claves públicas y privadas usada en el libro.

    b) Supón que no usamos certificados. Describe como Trudy se podría comportar como una “woman-in-the-middle”, interceptando los mensajes de Alice y haciendo creer a Bob que ella es Alice.

a)



b)



10. La aparición de la computación cuántica ha despertado mucha inquietud en el mundo de la criptografía. De hecho, la "Post-quantum cryptography" ya es un tema estrella en la literatura científica. Comenta porque la criptografía clásica se ve amenazada por la computación cuántica y busca información sobre la situación actual de la problemática.

Respuesta libre