# Prueba Corta 5 y 6

Estudiante: Jonder Hernández Gutiérrez
Carnet: 2018203660

## Preguntas

1. Autrum Transfer Protocol (ATP), es un protocolo creado durante los años 90 para el envío de mensaje (este utilizaba el puerto TCP/666), este se volvió muy popular entre las personas jóvenes de la época que tenían acceso a una red, este protocolo era capaz de transportar cualquier carácter visible ASCII, parte de lo emocionante de este protocolo era lograr enviar los mensajes de forma cifrada y el proceso era enteramente manual, lo cual quiere decir que las personas involucradas en la transmisión conocían las llaves para cifrar y descifrar mensajes. ATP se ha puesto de moda en el 2022, el problema es que ATP es un protocolo sumamente débil en términos de seguridad y además usa un puerto poco convencional como lo es TCP/666, con el fin de evaluar sí es posible implementar una versión segura de este protocolo, se le solicita responder las siguientes preguntas:
    - a. ¿Es posible enviar datos que no sean HTTPs sobre el puerto 443? Justifique su respuesta. (10 pts)
    - b. Suponiendo que creamos el protocolo ATP over SSL (ATPs), describa un subprotocolo para el establecimiento de una conexión SSL. (40 pts)
    - c. Si existe el protocolo ATPs, ¿Es posible transportar ATPs sobre HTTPs? Justifique su respuesta. (10 pts)
    - d. Desde un punto de vista de firewalls, ¿Porqué sería muy conveniente usar el puerto TCP/80 en lugar de puerto TCP/666?.
2. Explique detalladamente el funcionamiento de PKI. (30 pts)

## Respuestas

### 1. A

Si es posible enviar, como dice Tanenbaum "Cuando HTTP se utiliza encima de SSL, se conoce como HTTPS (HTTP Seguro), aunque es el protocolo HTTP estándar. Sin embargo, algunas veces está disponible en un nuevo puerto (443) en lugar de en uno estándar (80)" (Tanenbaum, 2003, p. 813).

Además de esto el puerto 443 no es diferente de otro puerto aparte de por su uso estandarizado por lo se puede usar sin problemas para conexiones SSL .

### 1. B

Para describir el subprotocolo se usará dos nombres ficticios: Alice y Bob.Para iniciar una conexión se comienza cuando Alice envía una solicitud a Bob para que establezca la conexión esta solicitud debe contener la versión SSL que tiene Alice y sus preferencias de algoritmos criptográficos y de compresión, además contiene una marca aleatoria $R_A$ .

Luego de esto Bob elige entre los algoritmos que Alice soporta y envía su marca aleatorio $R_B$. Luego de esto envía un certificado que contiene su llave pública.

Alice podra verificar la llave pública de Bob. En este punto Bob puede enviar algunos mensajes como por ejemplo solicitar el certificado de la clave pública de Alice. Cuando Bob termina envia a Alice una confirmación de que ahora es su turno.

Luego de esto Alice tiene que responder a Bob con una clave premaestra encriptada con su propia llave pública. Después de esto Alice le indica a Bob que cambie al nuevo cifrado y tambien que ha terminado con el establecimiento del subprotocolo.

Finalmente cuando Bob recibe la solicitud de cambio de cifrado cambia su cifrado y cuando recibe la confirmación del establecimiento del subprotocolo a su vez confirma el recibido por lo que finaliza tambien su establecimiento del subprotocolo (Tanenbaum, 2003, p. 837).

## 1. C

Si es posible transportarlo. Bastaría con empaquetar el mensaje del ATPs en el cuerpo del HTTPS y enviarlo.

## 1. D

En un Firewall el filtro de paquete de la LAN externa es el que verifica los paquetes entrantes, estos filtros son manejados por tablas configuradas por un administrador del sistema. Dentro de estas tablas se listan orígenes y destinos aceptables, orígenes y destinos bloqueados. Ya que el puerto 80 es uno de los puertos estándar más utilizados ya que sirve para publicar cualquier servicio web estándar, por esto mismo es muy probable que la tabla del filtro de LAN externa de la red donde se quiera entrar ya tenga como destino aceptable cualquier ip con el puerto 80. El puerto 666 casi no es usado por lo que seguramente la mayoría de Firewalls no van a tener el puerto 666 como puerto de destino aceptable (Tanenbaum, 2003, p. 799).

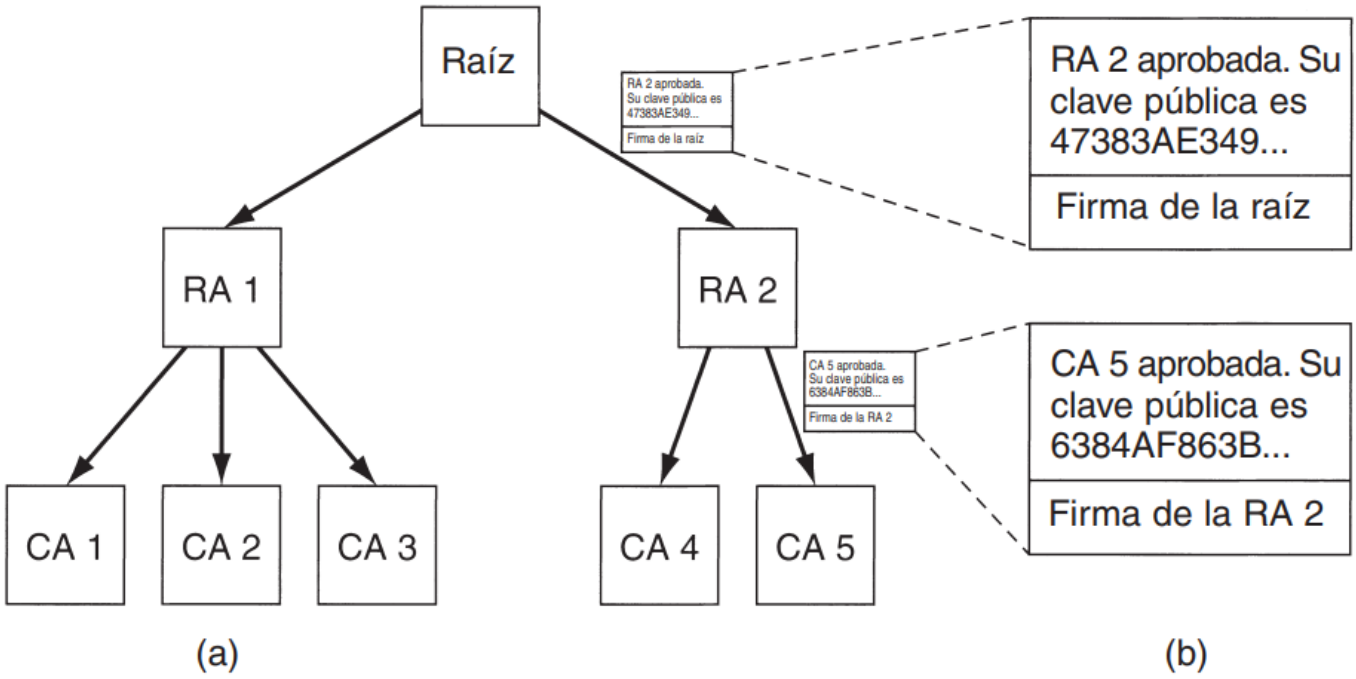
Por lo anterior podemos decir que si es más conveniente usar el puerto TCP/80 en lugar del TCP/666 por la facilidad de entrada que logra el puerto 80 al ser mucho más utilizado que el puerto 666 (Tanenbaum, 2003, p. 799).

## 2

Una PKI tiene múltiples componentes, entre ellos usuarios, CAs, certificados y directorios. PKI proporciona una forma para estructuras sus componentes y definir estándares. Una forma simple de PKI es una jerarquía de CAs, como se muestra en la Figura 1. A continuación podemos ver una descripción más a fondo de la estructura jerárquica de la Figura 1:

> La CA de nivel superior, la raíz, certifica a los de segundo nivel, llamaremos a estos RAs (Autoridades Regionales) debido a que podrían cubrir alguna región geográfica, como un país o un continente. Sin embargo, este término no es estándar; de hecho, ningún término es realmente estándar para los diversos niveles del árbol. Estás RAs, a su vez, certifican a los CAs reales, las cuales emiten los certificados X.509 a organizaciones e individuos. Cuando la raíz autoriza una nueva RA, genera un certificado X.509 donde indica que ha aprobado la RA, e incluye en él la nueva clave pública de la RA, la firma y se la proporciona a la RA. De manera similar, cuando una RA aprueba una CA, produce y firma un certificado que indica su aprobación y que contiene la clave pública de la CA Tanenbaum, 2003, p. 791).

Figura 1: (a) Una PKI jerárquica. (b) Una cadena de certificados.




Nota. De Tanenbaum [Figura], en Tanenbaum, A. Computer Networks.4ta edición. Upper Saddle River, NJ:Prentice Hall, 2003. P 769.

Para explicar la funcionalidad usaremos el siguiente ejemplo. Supongamos que Alice necesita una llave pública de Bob para comunicarse con él, por lo que encuentra un certificado firmado por la CA 5, sin embargo Alice no cree como fuente fiable la CA 5. Por lo que pide que se pruebe la autenticidad y esta responderá con un certificado que obtuvo de la RA 2, en la cual contiene la llave pública de la CA 5, después de esto Alice puede verificar que el certificado de Bob realmente fue firmado por la CA5 y que por lo tanto es verdadero. (Tanenbaum, 2003, p. 791).

## Referencias

1. Tanenbaum, A. Computer Networks. 4ta edición. Upper Saddle River, NJ:Prentice Hall, 2003