PC 9

Adriana López Calderón

2019293588

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:

- ¿Es posible enviar datos que no sean HTTPs sobre el puerto 443? Justifique su respuesta. (10 pts)

Es posible, este puerto proporciona un algoritmo de cifrado para intercambiar información entre servidores web y navegadores dedicado para la navegación web, este utiliza un certificado SSL/TLS para cifrar el texto original en un algoritmo y luego lo convierte en texto cifrado antes de enviarlo al servidor, aunque el protocolo predeterminado para el puerto 443 es HTTPS según el IETF, es posible enviar otro tipos de datos si están protegidos (encriptados) bajo SSL

- Suponiendo que creamos el protocolo ATP over SSL (ATPs), describa un subprotocolo para el establecimiento de una conexión SSL. (40 pts)

Un subprotocolo para crear la conexión SSL mediante un canal seguro, primero debe autenticarse o establecer una conexión entre el cliente y el servidor, la cual puede ser un mensaje que incluye una comprobación de la integridad del mismo usando una clave MAC, donde se intercambia la información de sesión tales como algoritmo a usar o id y de esta manera generar una o varias claves.

- Si existe el protocolo ATPs, ¿Es posible transportar ATPs sobre HTTPs? Justifique su respuesta. (10 pts)

Sí, debido a que HTTPS permite la transferencia de datos seguros que son encriptados sobre SSL y ATPs (ATP sobre SSL) que lo que busca es el envío de mensajes(caracteres) ya tendría la seguridad y/o encriptación requerida por HTTPS

- Desde un punto de vista de firewalls, ¿Porqué sería muy conveniente usar el puerto TCP/80 en lugar de puerto TCP/666?.

Ya que el puerto TCP/80 es un “Well-Known Port”, y el cual por lo general no se encuentra bloqueado por el firewall, por lo que es más sencillo de detectar y usar para los usuarios y cualquiera que lo apunte con un

navegador web podrá acceder fácilmente a él. Mientras que si utiliza un puerto no convencional como TCP/666 en la dirección deberá especificar dicho puerto de escucha para ser detectado

2.Explique detalladamente el funcionamiento de RSA. (30 pts)

Es un método de encriptación descubierto por un grupo de MIT. se implementa dividiendo el texto llano en bloques, para que cada mensaje de texto llano, P, caiga en el intervalo $0 \leq P < n$, luego agrupa el texto llano en bloques de k bits, donde k es el entero más grande para el que $2^k < n$ es verdad.

- Para encriptar un mensaje, P, se calcula $C = P^e \pmod n$.
- Para desencriptar C, se calcula $P = C^d \pmod n$.

Puede demostrarse que, para todos los P del intervalo especificado, las funciones de encriptación y desencriptación son inversas.Por otro lado, para ejecutar la encriptación, se necesitan e y n; y para llevar a cabo la desencriptación, se requieren d y n.