Escuela de Ingeniería en Computación

Redes IC-7602

Profesor: Nereo Campos

Estudiante: Mario Fernández Robert - 2018163975

Prueba corta #9

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)

      - Sí, es posible; sin embargo, no es recomendable, ya que se está rompiendo un estándar, además de utilizar un puerto bien conocido para enviar datos de una manera "no estándar".

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

      - El subprotocolo estaría basado en el three way handshake, primeramente se tienen 2 clientes que quieren establecer una conexión, el cliente1 enviaría un paquete con una petición de conexión, el cliente2 respondería enviando un paquete indicando que recibió la petición y que quiere establecer una conexión, finalmente el cliente1 enviaría un paquete confirmando la llegada del paquete del cliente2 y estableciendo una conexión, en el envío de estos 3 paquetes también se definirían las opciones y versión de SSL, además entre los clientes se deberán compartir sus respectivas llaves públicas.

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

      - Es posible, como en el caso del Ethernet por mensajes de texto y el transporte de información embebida en imágenes, es un caso muy similar, en el cual los caracteres ASCII pueden representarse como Bytes encriptarse y enviarse, para que el receptor reciba los Bytes y los desencripte con la respectiva llave.

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

    - El puerto TCP/80 es el puerto default, esto garantiza una aceptación de la conexión en prácticamente todos los casos, además al ser el puerto TCP/666 poco convencional pueden existir reglas de firewall que bloqueen la conexión.

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

Algoritmo de encriptación basado en teoría de números, que implementa los siguientes pasos:

- Definir los parámetros:
    - Se escogen 2 números primos de mínimo 1024 bits, es decir números primos muy grandes por encima del 50 000, a estos primos los llamaremos p y q
    - Calculamos n = p * q
    - Calculamos z = (p-1) * (q-1)
    - Escogemos un primo d con respecto a z tal que e * d = 1 mod z
- Algoritmo de Encriptación:
    - C = P^e (mod n)
- Algoritmo de Desencriptación:
    - P = C^d (mod n)