Tecnológico de Costa Rica

Ingenieria en Computación

IC-7602 - Redes - II Semestre 2022

Prueba Corta 9

Isaac David Ortega Arguedas | 2018189196

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)

    Sí, puede que no sea el puerto habitual, pero ya existen otros medios que utilizan este puerto para la comunicación. Este es un nuevo puerto el cual el protocolo HTTPs permite utilizar.

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

    El subprotocolo para establecer conexión SSL consta de 9 pasos. Un mensaje para solicitar conexión el cual especifica la versión SSL y preferencias con respecto a los algoritmos criptográficos y de compresión, así como una marca aleatoria, R_A. Luego el receptor envia un mensaje con una elección de entre los diversos algoritmos que el emisor puede soportar y envía su propia marca aleatoria, R_B. En el tercer mensaje el receptor envía un certificado que contiene su clave pública y, de ser necesario, también envía una cadena de certificados que pueden seguirse hasta encontrar uno. Una vez terminado esto envia el cuarto mensaje el cual le indica al emisor que es su turno.

    El emisor, con el quinto mensaje, responde eligiendo una clave premaestra aleatoria de 384 bits y enviándola al receptor encriptada con la clave pública de él. Posteriormente, el emisor, mediante el sexto mensaje, le indica al receptor que cambie al nuevo cifrado y también que ha terminado con el establecimiento del subprotocolo, esto mediante el mensaje siete. Después el receptor confirma que ha recibido la indicación esto serian los mensajes ocho y nueve.

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

    Sí. HTTP es un protocolo ASCII, lo que facilita que una persona hable con otra a traves de la web y HTTPs es el protocolo HTTP estándar el cual utiliza por encima el SSL.

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

  El puerto TCP/666 no es un puerto confiable, además de no ser un puerto común. Esto dos motivos podrian provocar que la mayoria de firewalls decida no permitir el acceso.

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

Cumple que dado $D(E(P)) = P$, si aplicamos D a un mensaje cifrado, E(P), obtenemos nuevamente el mensaje de texto llano original, P. Es excesivamente difícil deducir D de E y, E no puede descifrarse mediante un ataque de texto llano seleccionado Consta de cuatro etapas:E no puede descifrarse mediante un ataque de texto llano seleccionado. 1. Seleccionar dos números primos grandes, p y q (generalmente de 1024 bits). 2. Calcular n = p * q y z = (p - 1) * (q - 1). 3. Seleccionar un número primo con respecto a z, llamándolo d. 4. Encontrar e tal que e * d = 1 mod z.

Con estos parámetros calculados por adelantado, estamos listos para comenzar la encriptación. Dividimos el texto llano (considerado como una cadena de bits) en bloques, para que cada mensaje de texto llano, P, caiga en el intervalo $0 \leq P < n$. Esto puede hacerse agrupando 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, calculamos $C = P^e \pmod{n}$. Para desencriptar C, calculamos $P = C^d \pmod{n}$. Puede demostrarse que, para todos los P del intervalo especificado, las funciones de encriptación y desencriptación son inversas. Para ejecutar la encriptación, se necesitan e y n. Para llevar a cabo la desencriptación, se requieren d y n. Por tanto, la clave pública consiste en el par (e, n), y la clave privada consiste en (d, n).