Prueba Corta #9

Redes - IC-7602

Escuela de Ingeniería en Computación, ITCR

8-11-2022

Estudiante

- Zhong Jie Liu Guo - 2018319114

1. Se le solicita responder las siguientes preguntas:

   a. ¿Es posible enviar datos que no sean HTTPs sobre el puerto 443? Justifique su respuesta.

   Existe la posibilidad de usar el puerto 443 para enviar datos que no sean HTTPs, aunque este no es recomendado. Se debe a que múltiples aplicaciones web van a utilizar este puerto para establecer conexiones "seguras". Pero, al menos que ese puerto esté completamente reservado por la máquina que se va a usar, es posible usarla para otras tareas. Aún así, un programa puede no poder utilizar ese puerto ya que es de los puertos conocidos y se saben que se reservan para la tarea normal por protocolo o por la entidad que vela por los estándares.

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

   Podemos crear un subprotocolo igual al three way handshake donde tenemos a un emisor y un receptor. El emisor manda un paquete con la bandera SYN para querer establecer una conexión. Luego, el receptor manda un paquete con SYN-ACK para hacer saber que le llegó el mensaje al cliente y que se desea establecer esa conexión. Finalmente, el emisor manda un paquete con ACK para reafirmar la llegada de la respuesta y se establece la conexión entre ambos.

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

   Es completamente posible pasar ATPs en HTTPs ya que son bits los que van a pasar en las peticiones aunque sean encriptadas. Un caracter ASCII puede representarse por un byte, entonces se puede escribir en esa petición los bytes para luego extraerlos al otro lado de la petición.

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

   Como el protocolo ATP no la da mucha importancia a la seguridad, el puerto 80, protocolo http sería más conveniente de usar ya que tiene el mismo enfoque de la navegación sin "seguridad". En términos de firewall, las reglas para el uso del puerto 80 ya existen usualmente en las máquinas con navegación web, entonces no sería necesario declarar nuevas reglas para controlar el flujo de datos involucrados al puerto 666.

2. Explique detalladamente el funcionamiento de RSA.

El RSA es una algoritmo de encriptación asimétrico, es decir que ocupa de dos llaves: una pública y otra privada. Estas llaves van a ser de 1024 o 2048 bits y para escoger las llaves se escogen dos números primos grandes (**p**, **q**). La idea del RSA es que factorizar un entero grande es difícil por lo que la base van a ser esos dos números. Se calcula los valores **n = p * q** y **z = (p-1)*(p-1)**, se escoge un número primo **d** con respecto a z, luego se debe encontrar un **e** tal que **e * d = 1 mod z**. Para encriptar y desencriptar un mensaje **P** se utilizan las siguientes fórmulas:

- encriptar: `C = P^e (mod n)`
- desencriptar: `P = C^d (mod n)`