Tecnológico de Costa Rica
Escuela de Ingeniería en Computación
IC: 7602-Redes - 2 Semestre 2022
2018093728 - Paula Mariana Bustos Vargas

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:

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

No es posible enviar datos que no sean HTTPs sobre el puerto 443, debido a que esta asignado para la navegación web de manera segura.

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

Recordando que SSL consiste en dos subprotocolos, uno para establecer una conexión segura y otro para utilizarla. Se partira la explicacion partiendo del punto del subprotocolo de establecimiento de conexión y los usuarios Alice y Bob se tiene la siguiente comunicacion por mensaje

Alice -> Bob _____ Mensaje 1

- Comienza con el mensaje 1, cuando Alice envía una solicitud a Bob para que establezca una conexión. En esta solicitud se especifica:
    - la versión SSL que tiene Alice
    - Las preferencias con respecto a los algoritmos criptográficos y de compresión.
    - Una marca aleatoria, R(A), para utilizarse más tarde.

Bob -> Alice _____ Mensaje 2

- En el mensaje 2, Bob realiza una elección de entre los diversos algoritmos que Alice puede soportar y envía su propia marca aleatoria, R(B)

Bob -> Alice _____ Mensaje 3

- Bob, envía un certificado que contiene su clave pública

Bob -> Alice _____ Mensaje 4

- Bob envía en el mensaje 4 que ha terminado, para indicar a Alice que es su turno.

Alice -> Bob _____ Mensaje 5

- Alice responde eligiendo una clave premaestra aleatoria de 384 bits y enviándola a Bob encriptada con la clave pública de él
    - Alice como Bob pueden calcular la clave de sesión.

Alice -> Bob _____ Mensaje 6

- Alice indica a Bob que cambie al nuevo cifrado

Alice -> Bob _____ Mensaje 7

- Alice indica a Bob que ha terminado con el establecimiento del subprotocolo

Bob -> Alice _____ Mensaje 8

- Bob confirma el cambio de cifrado

Bob -> Alice _____ Mensaje 9

- Bob confirma la finalizacion del establecimiento del subprotocolo

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

Si ya que http (Protocolo de Transferencia de Hipertexto) es el protocolo de transferencia utilizado en World Wide Web y se sabe que se puede pasar diferentes tipos de contenidos a traves de este protocolo, como el profesor lo explico en el caso de transmision de diferentes paginas que estan encriptadas y se pasa por https.

Por lo que si se utilize el protocolo ATPs para el envio mensaje, asumiendo que tanto el emisor como receptor poseen la contraseña, el resultado de este mismo se podria mandar por https. Seria transporta un mensaje doblemente encriptado.

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

En si no existe gran diferencia entre un puerto y el otro ya que lo peligroso es tener un puerto abierto hacia un servicio de la capa de aplicación que no esté protegido, porque cualquiera se podría conectar a dicho servicio o hackearlo.

Dicho esto es más conveniente usar el puerto TCP/80 debido a que este puerto esta asignado por la Autoridad de Números Asignados de Internet (IANA) para la navegación del internet. Lo que lo hace un puerto convencional.

---

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

Su método se basa en ciertos principios de la teoría de los números.

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.

La clave pública consiste en el par (e, n), y la clave privada consiste en (d, n).

Con estos parámetros calculados por adelantado, se pasa a la encriptación.

- Se dividie el texto llano (considerado como una cadena de bits) en bloques, esto puede hacerse agrupando el texto llano en bloques de k bits, donde k es el entero más grande para el que 2 a la k < n es verdad.
- Para que cada mensaje de texto llano, P, caiga en el intervalo 0 ≤ P < n.
- Para poder encriptar P(mensaje) se calcula , calculamos C = (mod n) * P a la e
- Para desencriptar C, se calcula P = (mod n) * C a la d

La funcion de encriptar y desencriptar deben de ser inversas. La seguridad del método se basa en la dificultad para factorizar números grandes.

RSA requiere alguna forma de encadenamiento para la encriptación de datos. Su mayor desventaja es que requiere claves de por lo menos 1024 bitspara una buena seguridad (en comparación con los 128 bits de los algoritmos de clave simétrica), por lo cual es muy lento, para poder encriptar grandes volúmenes de datos, pero se utiliza con amplitud para la distribución de claves.