TRANSMISIÓN DE DATOS Y REDES DE ORDENADORES

Examen de Teoría[1]

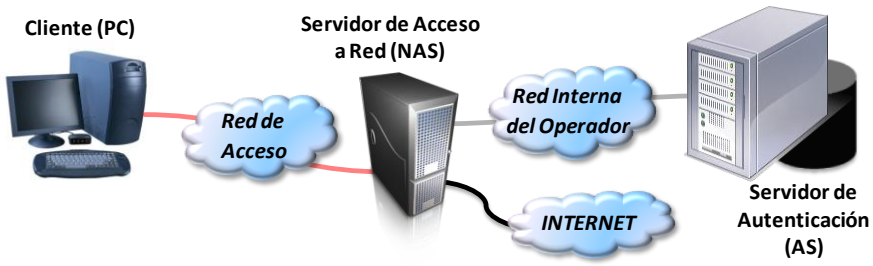
Septiembre de 2010

APELLIDOS, NOMBRE:

GRUPO TEORÍA:

---

1. (*2 puntos*) La figura y mensajes siguientes describen un hipotético protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.



PC → NAS: $Kpub_{NAS}$ (peticion_acceso + usuario)
NAS → PC: desafio
PC → NAS: $Kpub_{NAS}$(MD5(usuario:K_{PC-AS}:desafio))
NAS → AS: peticion_autenticacion + usuario + desafio + MD5(usuario:K_{AS-PC}:desafio))
AS → NAS: peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
(ó peticion_rechazada)
NAS → PC: $Kpriv_{NAS}$ (peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$))
(ó $Kpriv_{NAS}$ (peticion_rechazada))
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar)
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC-NAS}$ (datos_de_respuesta)

Siendo:

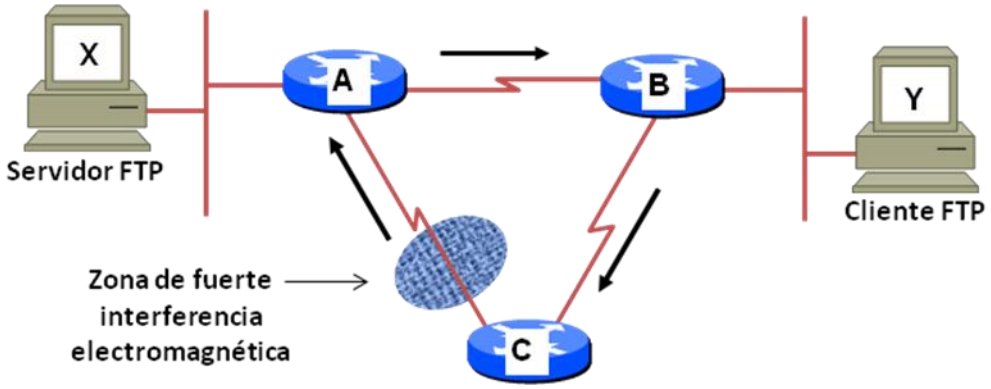
- $Kpub_X$ cifrado con la clave pública de X
- $Kpriv_X$ cifrado con la clave privada de X
- K_{X-Y} la clave secreta entre X e Y
- MD5 es una función *hash*

Aceptadas la disponibilidad y validez de las claves públicas involucradas en base a la existencia de una entidad superior confiable, responda razonadamente:

a) ¿Qué servicios de seguridad se proporcionan en el protocolo descrito?
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

[1] Esta prueba supone el 70% de la calificación final de la asignatura.

2. (*2 puntos*) En la red de la siguiente figura Y ha establecido con X una conexión FTP (sobre TCP) y ha solicitado el envío de un fichero que para transmitirse requiere el envío de 20 segmentos. No se envían datos en sentido contrario, por lo que el TCP de Y solo envía a X los ACKs correspondientes:



Como muestra la figura la comunicación utiliza rutas asimétricas. Además, el enlace entre los routers A y C pierde una de cada tres tramas que pasan por él (es decir, falla la tercera, la sexta, etc.).

Suponga que no hay problemas de congestión, no hay control de flujo y la ventana de congestión inicial es igual a 2 MSS.

a) Describa la secuencia de segmentos que intercambiarán las capas TCPs de X e Y, detallando los envíos duplicados que se produzcan (si es que se producen). Omita la parte correspondiente al establecimiento y terminación de la conexión TCP.

b) Calcule el tiempo necesario para transferir el fichero suponiendo que el RTT de la comunicación X-Y es igual a 100 ms y que el timeout de retransmisión es de 200 ms. Considera despreciable el tiempo que se tarda en emitir los segmentos por las interfaces.

3. (1 puntos) Desde un ordenador se arrancan tres navegadores diferentes, Internet Explorer, Mozilla Firefox y Google Chrome, y se accede desde los tres a un servidor web en la dirección 147.156.1.4 (el mismo desde los tres) ¿Cuántos sockets y cuantas conexiones TCP están implicados, tomando en cuenta tanto el lado servidor como el cliente?

4. (1 puntos) ¿Qué significa el campo TTL de los RR (Registros de Recursos) de un paquete DNS?

5. (1 puntos) Una empresa tiene cinco departamentos, cada uno con una subred con direcciones privadas. Los rangos que elige el administrador de red son los siguientes:

- Departamento 1: 192.168.0.0/25
- Departamento 2: 192.168.0.128/27
- Departamento 3: 192.168.0.160/26
- Departamento 4: 192.169.0.0/25
- Departamento 5: 192.169.0.128/25

Explique detalladamente dos posibles problemas que tenga esta asignación.