

(66.62) REDES DE COMPUTADORAS		1999	
PRÁCTICA Número:	11	TEMA:	Repaso de Seguridad

IMPORTANTE: En las preguntas con opciones () , puede haber una, más de una o ninguna, opción verdadera. Tilde () la o las opciones que a su juicio resulten verdaderas.

1. Si luego de un estudio se concluye que un sistema dado cumple con las condiciones establecidas por el modelo Bell-LaPadula,

en principio, el sistema será inmune al accionar de espías que no tengan acceso a los niveles superiores

en principio, el sistema será inmune a la acción de “caballos de troya” colocados en niveles inferiores.

está asegurado que el sistema no tiene canales encubiertos (covert channels)

2. (1) DES en modo Cyclic Block Chaining se puede utilizar

para cifrar mensajes de más de 8 bytes

para firmar un mensaje usando un sistema simétrico.

para aumentar la seguridad de DES en modo ECB

3. (1) Porqué se utiliza un sistema simétrico junto con uno de clave pública ?

Porque el de clave pública no sirve para encriptar.

Porque no es sencillo distribuir la clave en el simétrico.

Porque el de clave pública es muy lento cifrando

4.(1) Cómo se puede asegurar que sólo el destinatario conozca el contenido de un mensaje ?

Cifrando su contenido con la clave pública del destinatario .

Cifrando su contenido con la clave privada del remitente

Calculando un hash del mensaje y transmitiéndolo.

5.(1) Cómo se puede firmar digitalmente un documento ?

Calculando un hash y transmitiéndolo junto con el mensaje.

Cifrando un hash de su contenido con la clave pública del destinatario .

Cifrando la clave pública del destinatario con la clave privada del remitente

6. (1) Cómo podría un eventual atacante tener acceso al contenido de un mensaje encriptado correctamente (encriptado para asegurar privacidad)?

Reemplazando el certificado del remitente previamente al cifrado.

Reemplazando el certificado del destinatario previamente al cifrado.

Reemplazando el mensaje por otro.

7.(1) SSL (Secure Sockets Layer) es un protocolo criptográfico

de tipo enlace-por-enlace (link-by-link).

de tipo punta a punta (end-to-end).

pero no encripta, sólo provee autenticación

(66.62) REDES DE COMPUTADORAS		1999	
PRÁCTICA Número:	11	TEMA:	Repaso de Seguridad

8. (1) Qué puede usarse para facilitar la administración remota de servers a través de la internet ? .

- TCP wrappers.
- SSL.
- S/Key

9. (1) Cómo se puede evitar el acceso al servicio telnet de un host por parte de un cliente, si ambos estan separados por un firewall ?

- Colocando un filtro que impida el tráfico entrante dirigido a la puerta 23 de TCP.
- Colocando un filtro que impida el tráfico saliente originado en la puerta 23 de TCP.
- Colocando un filtro que impide todo tráfico TCP saliente del firewall

10. (1) Cómo se puede evitar el acceso al servicio telnet de un host por parte de un cliente, si ambos estan **del mismo lado** de un firewall ?

- Utilizando un TCP wrapper.
- Colocando el servicio telnet en otro número de port, distinto del 23.
- Utilizando S/Key