Universidad de Granada
Departamento de Teoría de la Señal,
Telemática y Comunicaciones

SEGURIDAD EN REDES DE COMUNICACIÓN

– 3er. curso Grado en Ingeniería de Tecnologías de Telecomunicación –

Examen de teoría[1] – Septiembre 2015

Apellidos: _____ **Nombre:** _____

1. *(1 pto.=2×0,5)* Considere la siguiente técnica de autenticación de doble sentido:

1. A → B: ID_A
2. B → A: R_1
3. A → B: R_2
4. B → A: $K_{AB}(R_2)$
5. A → B: $K_{AB}(R_1)$

a) Explique el esquema en cuestión y un ataque al que es susceptible.

b) Modifique mínimamente el procedimiento para evitar el ataque mencionado.

[1] Las respuestas deben limitarse al espacio reservado para ello.

2. *(1 pto.=4×0,25)* Suponga el mensaje M generado a partir de uno P, por un emisor A para su envío a un receptor B:

$$M = \underset{1}{RSA\text{-}K_{prA}}\left(\underset{2}{RSA\text{-}K_{puB}}\left(P + \underset{3}{HMAC\text{-}K_{AB}}(P) \right) \right)$$

Responda a las siguientes cuestiones:

a) ¿Se proporciona confidencialidad? En caso afirmativo, ¿mediante cuál de las 3 operaciones efectuadas sobre P?

b) ¿Se proporciona integridad? En caso afirmativo, ¿mediante cuál de las 3 operaciones efectuadas sobre P?

c) ¿Se proporciona disponibilidad? En caso afirmativo, ¿mediante cuál de las 3 operaciones efectuadas sobre P?

d) ¿Cree que alguna de las operaciones realizadas es redundante desde el punto de vista del servicio ofertado? Justifique brevemente la respuesta.

3. *(1 pto.=4×0,25)* Describa las claves que se indican a continuación en relación con un sistema IEEE 802.11i, señalando si son paritarias o de grupo:

PSK:

PMK:

GMK:

GTK:

4. *(1 pto.=2×0,5)* Responda a las siguientes cuestiones sobre el protocolo PPTP:

a) Esquematice el encapsulado/túnel realizado. ¿Cómo se lleva a cabo el control del túnel?

b) ¿Qué tipos de mensajes principales contempla el protocolo? Indique al menos uno de los mensajes existentes para cada tipo.

5. *(0,5 ptos.)* Discuta la siguiente afirmación:

Un sistema de detección de incidentes de seguridad (virus, troyanos, intrusiones, etc.) es mejor cuanto mayor sea su tasa de detección de eventos maliciosos

6. *(1,5 ptos. =3×0,5)* Responda a las siguientes cuestiones sobre el protocolo IPsec:

a) ¿Qué servicios de seguridad proporciona? ¿Mediante qué procedimiento en cada caso?

b) Esquematice la arquitectura de seguridad asociada, indicando el fin de cada elemento.

c) Explique el intercambio de mensajes involucrado en la etapa inicial, según el siguiente esquema: