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] – Junio 2016

Apellidos: _____ **Nombre:** _____

1. *(1,5 ptos.=3×0,5)* Supuesta una red IEEE 802.11i basada en *WPA2 Enterprise*, responda:

a) ¿Qué algoritmos de cifrado, integridad y autenticación utiliza?

b) Indique el conjunto de claves paritarias usado, así como el árbol de dependencias relativo a su generación. ¿Cuál de ellas es la usada para proporcionar confidencialidad en las comunicaciones estación-AP?

c) Esquematice de forma gráfica el proceso de autenticación involucrado en el sistema, especificando las entidades implicadas.

[1] Esta parte de la asignatura se evaluará sobre un máximo de 6 puntos, debiéndose responder a cada una de las preguntas/ejercicios en el espacio específico reservado para ello.

2. *(2 ptos. = 1+2×0,5)* Al respecto del algoritmo de cifrado AES:

a) Explique de forma breve los cuatro procesos implicados en cada una de las rondas del procedimiento:

SubBytes

ShiftRows

MixColumns

AddRoundKey

b) Conteste de forma concisa a las siguientes cuestiones:

i. ¿Qué longitud de bloque (en bits) de entrada se usa en AES?

ii. ¿Cuál es la longitud (en bits) del bloque de salida?

iii. ¿Cuál es la longitud (en bits) de clave superior considerada en AES?

iv. ¿Cuántas rondas sucesivas se realizan en este último caso?

v. ¿Cuántas claves y de qué longitud se usan en el proceso *AddRoundKey* en cada ronda?

c) Indique una ventaja y una limitación del modo *CTR* frente al *CBC* para este algoritmo de cifrado.

3. *(1 pto. = 4×0,25)* En relación al protocolo PPTP en VPN:

a) Indique dos de los campos de la cabecera de los mensajes PPTP.

b) ¿Cuántos tipos de mensajes existen y para qué se utilizan? Indique un sub-tipo, en su caso, de cada uno de los tipos.

c) ¿Qué tipo de túnel de nivel 3 utiliza?

d) Esquematice, indicando las distintas cabeceras y *payload*, el encapsulado de PPP realizado.

4. *(1,5 ptos. =15×0,1)* Marque la respuesta correcta a cada cuestión *(cada incorrecta resta 0,025 ptos.)*:

a)	**Un ataque de *man-in-the-middle* actúa contra**	
	La confidencialidad	☐
	La autenticación	☐
	La disponibilidad	☐
	Todos los aspectos antes mencionados de la seguridad	☐
b)	**La robustez de un algoritmo de cifrado debe radicar en**	
	La ocultación pública de los diferentes procedimientos de sustitución y/o transposición que lo componen	☐
	El uso de protocolos de autenticación fiables	☐
	La consideración de políticas de seguridad que sigan el estándar X.800	☐
	La robustez (y privacidad) de la clave usada	☐
c)	**El algoritmo de Diffie-Hellman**	
	Es de tipo asimétrico	☐
	Precisa el conocimiento a priori de la clave	☐
	A diferencia de RSA, basa su potencia en la teoría de los números primos	☐
	Todas las respuestas anteriores son incorrectas	☐
d)	**Las funciones *hash***	
	Permiten la integridad de los mensajes	☐
	Generan un resumen del mensaje de tamaño fijo y único para el mismo	☐
	Son de un solo sentido (*one-way*)	☐
	Todas las respuestas anteriores son correctas	☐

e)	**Una firma digital es**	
	El cifrado de la función compendio de un mensaje	☐
	Los datos de identificación proporcionados por una entidad certificadora	☐
	La digitalización de un documento privado	☐
	El cifrado del mensaje intercambiado entre un emisor y un receptor	☐
f)	**Un certificado X.509 contiene, entre otra información, la siguiente:**	
	Algoritmo de cifrado y clave privada a usar entre el usuario y la entidad certificadora	☐
	Dirección IP y DNI del usuario	☐
	Clave privada de la entidad emisora del certificado	☐
	Identidad del usuario y clave pública de éste	☐
g)	**La cabecera AH de IPSec en modo túnel se encapsula como sigue:**	
	Cabecera_IP2 + AH + Cabecera_IP1 + Datos	☐
	Cabecera_IP + AH + Datos	☐
	AH + Cabecera_IP1 + Cabecera_IP2 + Datos	☐
	Cabecera_IP1 + Cabecera_IP2 + AH + Datos	☐
h)	**Una asociación de seguridad está formada por**	
	SPI + dirección_IP	☐
	SPI + AH/ESP	☐
	SPI + dirección_IP + AH/ESP	☐
	SPI + dirección_IP + Puerto_local + Puerto_remoto	☐
i)	**En el protocolo *Record* de TLS**	
	Los mensajes se fragmentan en bloques	☐
	Se utiliza RSA como algoritmo de cifrado	☐
	Se implementa MD5 como procedimiento de autenticación de los mensajes	☐
	Todas las respuestas anteriores son correctas	☐
j)	**El mensaje *SSH_MSG_CHANNEL_DATA* es propio del protocolo**	
	TLP de SSH	☐
	CP de SSH	☐
	UAP de SSH	☐
	CCP de SSH	☐
k)	**Un cortafuegos *proxy* o de aplicación, frente a uno de filtrado o IP,**	
	Limita el número de puertos abiertos en una máquina	☐
	Mantiene y comparte el estado con la información de las comunicaciones existentes	☐
	Establece, llegado el caso, una comunicación indirecta entre las partes involucradas	☐
	Todas las respuestas anteriores son correctas	☐
l)	**La principal diferencia entre un *gusano* y cualquier otro *malware* radica en que**	
	Un gusano tiene capacidad de auto-propagación	☐
	Sólo los gusanos son replicables	☐
	Resultan indetectables	☐
	No presentan fase de *disparo*	☐
m)	**Una técnica de detección de cualquier *malware* es**	
	Detección de actividades normales en el entorno	☐
	Determinación de una tasa de paquetes servidor→cliente elevada	☐
	Uso de firmas/patrones identificativos	☐
	Generación de reglas de reenvío en el cortafuegos	☐
n)	**Las técnicas de *watermarking***	
	Son tecnologías denominadas ERM/IRM, donde se trata de controlar el recurso distribuido	☐
	Implican una autenticación *online* del usuario	☐
	A diferencia de las técnicas de *fingerprinting*, incorporan datos del consumidor del producto	☐
	Todas las respuestas anteriores son incorrectas	☐
ñ)	**El término *cibercrimen* se refiere a:**	
	Ataque contra páginas web	☐
	Fraude contra una entidad bancaria	☐
	Asesinato simulado a través de YouTube	☐
	Delito cometido mediante el empleo de herramientas informáticas	☐