Examen-Febrero-2018-RESUELTO.pdf

Juandf03

Seguridad de la Información

3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga

 # Parte 1

****1. Describir las características en las que radica la fortaleza del cifrado OTP.****

El cifrado OTP (One Time Pad) tiene la característica de que es de un solo uso, por lo que una vez utilizado para cifrar/descifrar un mensaje, será encesario otra lista de caracteres (pad); esto favorece a la seguridad ya que no puede cifrarse/descifrarse un mensaje con pads distintos y obtener el mismo resultado.

****2. Explicar las diferencias esenciales entre los algoritmos de cifrado en bloque y los de cifrado en flujo.****

Los algoritmos de cifrado en bloque requieren dividir el mensaje en subcadenas -bloques- de una longitud específica, de forma que se cifra cada uno de esos bloques y al final, se concatenan todos ellos obteniendo así el mensaje cifrado. Sin embargo, los algoritmos de cifrado en flujo cifran el mensaje bit a bit, habiendo generado previamente una cadena aleatoria de bits (con la que operar mediante la operación XOR).

****3. Definir qué es el efecto avalancha. Explicar en qué conceptos básicos de la Teoría de la Información se basa ese efecto.****

Se denomina «efecto avalancha» al hecho de producir cambios significativos en el mensaje cifrado con cambios pequeños en el mensaje en claro o la clave.

Se basa en los conceptos de confusión y difusión.
* Confusión: La relación entre el texto cifrado y la clave debe ser lo más complicada posible.
* Difusión: Cada caracter del texto cifrado debe depender de alguna parte de la clave.

****4. Describir brevemente las ventajas de los algoritmos de clave pública respecto a los algoritmos simétricos. Justificar la existencia/uso de los criptosistemas híbridos.****

Cuando 2 usuarios se comunican, no necesitan aclarar una clave a priori; lo que implica que no resulte problemático que estén lejanos físicamente; y por último, el número de claves se reduce de _*(n * (n-1) / 2)*_ en los algoritmos simétricos a _*2*n*_ en los algoritmos asimétricos, donde n es el número de usuarios de la comunicación.

Los criptosistemas híbridos combinan algoritmos simétricos con asimétricos, y se usan debido a su bajo rendimiento: 2 usuarios usan un algoritmo asimétrico para el intercambio de una clave que usarán posteriormente para cifrar su comunicación mediante un algoritmo simétrico. Se usa

el más pesado (asimétrico) una sola vez, para asegurar una comunicación con el cifrado más ligero (simétrico).

****5. Describir las características principales de una función hash criptográfica. ¿Tiene sentido usar una función de este tipo en combinación con el algoritmo Diffie-Hellman?****

Una función hash transforma un bloque de información de longitud variable *_M_* en un bloque de información hash de longitud fija *_h_* (huella digital de *_M_*): la función es unidireccional, ya que con *_h_*, no puede obtenerse *_M_*; y también libre de colisiones, porque es imposible que 2 mensajes *_M_* y *_M'_* distintos produzcan el mismo *_h_*.

****6. Definir los 5 servicios básicos de seguridad definidos por ISO 7498-2 e ITO X.800.****

* Confidencialidad: protección de los datos frente a aquellos que no deben acceder a ellos.
* Autenticación: asegurarse de que la entidad con la que me comunico es realmente quien dice ser.
* Integridad: asegurarse de que los datos que recibo son realmente los que se han enviado.
* No repudio: protección contra la negación de hechos de entidades de la comunicación.
* Control de acceso: prevención del uso no autorizado de información o un recurso.

 # Parte 2

****1. Completar las siguientes oraciones.****

* Los protocolos *WEP y WPA* proporcionan autenticación a nivel de red.

* IKE se caracteriza por aplicar protocolos concretos para las negociaciones de las asociaciones de seguridad junto con las claves de sesión. Uno de ellos es: *ISAKMP*.

* SSL proporciona varios servicios de seguridad, menciona al menos 2: *autenticación al servidor* e *integridad a los datos*.

* La combinación de los algoritmos de intercambio de clave, cifrado y hash define un *cipher suite* para cada sesión SSL.

* SET proporciona un conjunto de servicios de seguridad, mencionar al menos 4: *Autenticidad, privacidad, integridad y reducción de disputas*.

* Los sistemas basados en proxy, nodos mixers o routers onions siguen arquitecturas *centralizadas*, mientras que los sistemas basados en Crowds o Hordes se basan en arquitecturas *distribuidas o de grupos*.

McDonald's

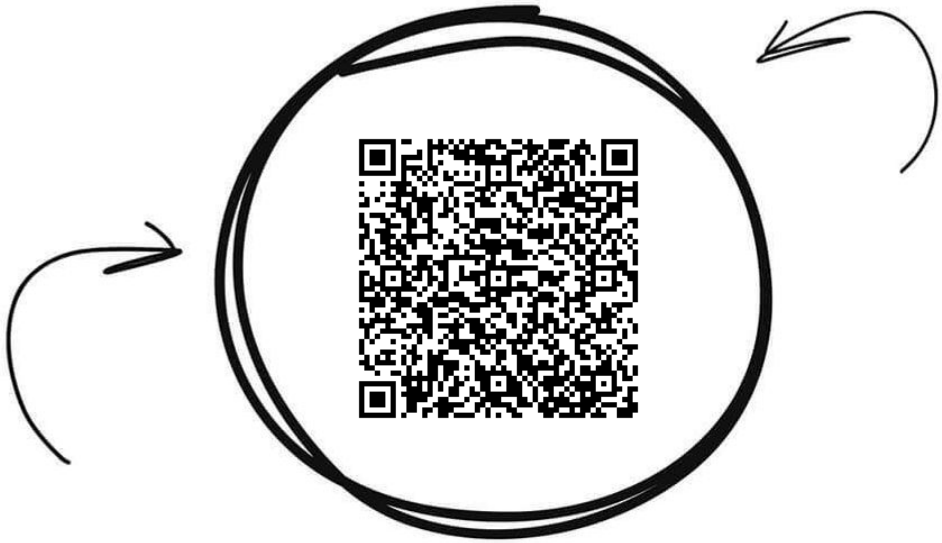
“SOY CREW DE McDONALD’S, Y POR SUPUESTO QUE MI TRABAJO Y MI PASIÓN SON COMPATIBLES”

¿TE VIENES?

My CREW

Mi trabajo. Mi pasión. Mi gente.

Seguridad de la Información



Banco de apuntes de la

WUOLAH

Comparte estos flyers en tu clase y consigue más dinero y recompensas

1. Imprime esta hoja
2. Recorta por la mitad
3. Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes
4. Llévate dinero por cada descarga de los documentos descargados a través de tu QR

2. Responde con Verdadero o Falso las siguientes preguntas y argumenta tu elección.

* Tanto SSL como TLS proporcionan servicios de comprensión desde la capa de aplicación.

* Cualquier protocolo criptográfico puede ser aplicado para implementar los protocolos de lanzamiento de moneda y de póker mental.
  * Falso: solo los protocolos con Confirmación de Bit.

* Millicent garantiza anonimato al comprador.
  * Falso: gracias a su modelo se consigue cierto anonimato, pero no completo. El agente sabe la identidad del comprador y su número de tarjeta, pero no el producto; mientras que el vendedor sabe el producto, pero no la identidad del comprador.

* Con `iptables_A INPUT-s 0.0.0.0/0 –p tcp—dport 25 –j ACCEPT`, se especifica que el firewall solo permite trafico telnet entrante.

3. Completar la siguiente tabla respecto a qué cabeceras usar según los servicios que queramos proporcionar:

	AH	ESP (sin autenticación)	ESP (con autenticación)
Confidencialidad			
Autenticación			
Integridad			
Control de paquetes reenviados			
No repudio			

4. Representar el esquema o diagrama de transmisión de mensajes PGP -tanto por parte del emisor como por parte del receptor- de forma que se especifique claramente qué servicios son obligatorios y cuáles son opcionales.

Transmisión:

1. Seleccionar archivo.
   * ¿Necesita firma digital? -> Generar la firma y concatenarla con el archivo.
2. Comprimir el archivo.
   * ¿Necesita confidencialidad? -> Cifrar el mensaje.
3. Convertir a *radix 64*.

Recepción:

1. Desconvertir de *_radix 64_*.
   * ¿Necesita confidencialidad? -> Descifrar el mensaje.
2. Descomprimir el archivo.
   * ¿Necesita firma digital? -> Extraer la firma digital del mensaje.
3. Obtener el archivo.

****5. Sea el protocolo Otway-Rees:****

1. Dibuja y explica los agujeros de seguridad en el protocolo.

```
1. A -> B : I, A, B, Eat(I, A, B, Na)
2. B -> T : I, A, B, Eat(I, A, B, Na), Ebt(I, A, B, Nb)
3. T -> B : I, Eat(Kab, Na), Ebt(Kab, Nb)
4. B -> A : I, Eat(Kab, Na)
```

El protocolo cuenta con 2 agujeros de seguridad importantes:
* Si un atacante se hace pasar por el receptor del mensaje y la longitud de *_I_* || *_A_* || *_B_* coincide con la longitud de la clave *_Kab_*, dicho atacante puede reenviarle el mensaje.
* Si un atacante se hace pasar por el TTP y la longitud de *_I_* || *_A_* || *_B_* coincide con la longitud de la clave *_Kab_*, dicho atacante puede reenviar los mismos mensajes a *_A_* y a *_B_*.

2. Dibuja y explica una posible solución de tu elección.