Redes de Comunicaciones 2
25 de abril de 2022
MODELO 2

1. Imagina un cifrador de bloque que opera a nivel de byte y utiliza un modo de encadenamiento CBC, con IV = 0xAF. Para un texto en claro m = 0xCB0478, ¿cuál sería la entrada a la etapa de cifrado del primer bloque?
    a) 0xAB
    b) 0xAF
    c) 0x13
    d) 0x64

2. ¿Con qué elemento se firma un certificado digital?
    a) La clave privada de la Autoridad de Registro
    b) La clave privada de la Autoridad de Certificación
    c) La clave pública de la Autoridad de Certificación
    d) La clave pública de la Autoridad de Registro

3. Dada la siguiente configuración del firewall de un router doméstico, ¿cuál de las siguientes afirmaciones es cierta?

Action	Source Address	Dest. Address	Protocol	Source Port	Dest Port
Allow	192.168.0.31	91.198.174.192	TCP	Any	80
Allow	192.168.0.31	91.198.174.192	TCP	Any	443
Deny	192.168.0.31	Any	TCP	Any	Any

    a) Únicamente permite navegar desde el ordenador con IP 192.168.0.31.
    b) Sólo el ordenador con IP 192.168.0.31 puede navegar, y sólo puede hacerlo al servidor Web con IP 91.198.174.192.
    c) Cualquier ordenador local, menos el que tiene IP 192.168.0.31, puede navegar a cualquier sitio.
    d) El ordenador con IP 192.168.0.31 puede contactar al servidor Web con IP 91.198.174.192, pero no puede recibir respuesta.

4. Dado un mensaje de Bob a Alice, ¿cuál de las siguientes operaciones permite asegurar la confidencialidad de la información, pero **no** su integridad?
    a) Enviar el hash del mensaje, cifrado con la clave pública de Bob
    b) Enviar el hash del mensaje, cifrado con la clave privada de Bob
    c) Cifrar el mensaje con la clave privada de Alice y enviar el hash del mensaje cifrado con la clave privada de Bob
    d) Cifrar el mensaje con la clave pública de Alice.

5. Supón que Alice recibe un mensaje de Bob, para el que se supone que tiene garantizadas la confidencialidad y la integridad. ¿Qué operaciones debe ejecutar Alice para leer el mensaje y tener la seguridad que ha sido escrito por Bob?
    a) Descifrar el mensaje con su clave privada, calcular el hash del mensaje y comprobar si ese hash es igual al valor obtenido al descifrar la firma del mensaje con la clave pública de Bob.
    b) Descifrar el mensaje con su clave pública, calcular el hash del mensaje y comprobar si ese hash es igual al valor obtenido al descifrar la firma del mensaje con la clave pública de Bob.
    c) Descifrar el mensaje con su clave privada, calcular el hash del mensaje y comprobar si ese hash es igual al valor obtenido al descifrar la firma del mensaje con la clave privada de Bob.
    d) Descifrar el mensaje con su clave privada, calcular el hash del mensaje, cifrar ese hash con la clave pública de Bob y comprobar el valor obtenido coincide con la firma del mensaje enviada por Bob.

Redes de Comunicaciones 2
25 de abril de 2022
MODELO 2

6. ¿Cuál de estas afirmaciones sobre el cifrado simétrico y asimétrico es correcta?
    a) El cifrado asimétrico es más eficiente y seguro, pero sólo sirve para enviar mensajes relativamente cortos (longitud menor que n)
    b) El cifrado simétrico es más seguro y eficiente que el asimétrico, pero tiene el problema de requerir un método adicional para compartir la clave.
    c) El cifrado asimétrico es más eficiente y seguro, el problema está en tener que calcular cada vez un par de claves pública-privada
    d) El cifrado simétrico es más eficiente, pero es más fácil de romper a través de métodos de fuerza bruta.
7. Usando el cifrado por bloque CBC, si Bob no recibe el vector de inicialización (VI):
    a) No podrá descifrar el primer bloque del mensaje enviado por Alice, pero sí el segundo y sucesivos.
    b) No podrá descifrar los dos primeros bloques del mensaje enviado por Alice, pero si el tercero y sucesivos.
    c) Podrá descifrar todos los bloques del mensaje enviado por Alice siempre y cuando tenga la clave correcta.
    d) No podrá descifrar ningún bloque del mensaje enviado por Alice.
8. ¿Cuál de estas afirmaciones sobre el protocolo Diffie-Hellman es verdadera?
    a) Por sí solo permite garantizar la confidencialidad del intercambio de mensajes.
    b) Por sí solo permite garantizar la confidencialidad del intercambio de mensajes.
    c) Utilizado para cifrar una clave simétrica permite garantizar la confidencialidad de los mensajes.
    d) Utilizado para cifrar una clave simétrica permite garantizar la integridad y autenticidad de los mensajes.
9. Respecto de la vulnerabilidad conocida del método de cifrado WEP 802.11:
    a) El atacante puede descubrir la clave a partir del vector de inicialización y lograr que el emisor cifre un texto conocido.
    b) La forma de evitar esta vulnerabilidad es cifrar el vector de inicialización.
    c) Como el vector de inicialización se usa sólo al principio de la comunicación, para tener éxito un atacante debe interceptar la comunicación desde el primer momento.
    d) Para evitar este problema, el transmisor crear un vector de inicialización de 24bits en cada sesión.
10. ¿Cuál de las siguientes afirmaciones sobre el funcionamiento de antivirus, firewalls e IDSs es correcta?
    a) Como los IDSs y los antivirus funcionan con el mismo método (búsqueda de patrones considerados maliciosos), en general no tiene sentido combinar el uso de antivirus e IDS en una red de ordenadores.
    b) Normalmente, independientemente del tipo de IDS, se instala uno por cada ordenador que debe ser protegido.
    c) La ventaja de un IDS respecto de un firewall es que, aunque ambos analicen paquetes, el IDS lo puede hacer sobre todo el historial de paquetes transmitidos y sólo sobre paquetes individuales.
    d) La ventaja de un IDS respecto de un firewall es que debemos instalar un firewall en cada ordenador a proteger, mientras que un IDS puede proteger un conjunto de ordenadores (una subred, por ejemplo).