Depto. Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid
ETSI Telecomunicación

Seguridad en Sistemas y Redes de Telecomunicación

Examen – 11.1.2019

Si considera que el enunciado es ambiguo, complételo de forma razonada.
En la corrección se valorará el razonamiento.

1. Ejercicio 1 (valor: 1/3)

Dos empresas desean intercambiar unos *streams* de video bastante voluminosos (gigabytes). Para ello han establecido una clave secreta común k.

El problema que tienen es que los datos están estructurados de forma muy rígida y repetitiva y preguntan qué modo de cifrado les conviene. Debido al hardware de qué disponen, tiene que ser uno de entre ECB, CBC o CTR.

Como circunstancia especial, sabemos que los atacantes intentarán modificar el primer bloque del mensaje a transmitir (M0, si el *stream* está formado por los bloques M0, M1, M2, etc.). Es decir, que el atacante lo quiere cambiar M0 por M0', sin conocer M0. ¿Podrá hacerlo?

Describa:

1. Ventajas e inconvenientes de usar el modo ECB (Electronic codebook)
2. Ventajas e inconvenientes de usar el modo CBC (Cipher Block Chaining)
3. Ventajas e inconvenientes de usar el modo CTR (Counter)

Suponga que el atacante conoce y puede modificar el vector inicial IV en los modos que lo usan.

2. Ejercicio 2 (valor: 1/3)

Tenemos una red de dispositivos IoT (Internet of Things) en una zona donde queremos establecer un canal cifrado común para todos ellos; es decir, que las comunicaciones sean tipo broadcast donde todo el mundo lo oye todo, pero solo los que poseen la clave K acordada pueden entender los mensajes radiados.

Para ello, en la fase de inicialización, cargamos en cada dispositivo un valor aleatorio R, común a todos los dispositivos. Uno de los dispositivos funciona como *master* (M). M, periódicamente, emite un número n. Los dispositivos escuchan M y establecen como clave de grupo el hash n-ésimo de R. O sea

$$K = H^n(R)$$

K se usa como clave de un cifrado simétrico; por ejemplo, AES.

1. Indique qué tamaño mínimo debe tener R y K. Además, si H proporciona X bits, indique como extraer los bits para K. Considere tanto el caso de que H genera más bits que los que necesita K, y el contrario, que genera menos.

2. ¿En qué modo de cifrado pondremos a trabajar el algoritmo AES para transmitir una gran cantidad de datos (por ejemplo, el *video streaming* de una cámara)?
3. Estamos preocupados por la PFS (Perfect Forward Secrecy). Describa en qué consiste la preocupación y qué cautelas debemos tomar para proporcionar PFS.
4. Estamos preocupados por la posible suplantación del *master* M por otro dispositivo M'. Esta suplantación puede ser deliberada (buscada por un atacante) o accidental (solape radio de zonas IoT diferentes). ¿Qué consecuencias podría tener una suplantación? ¿Cómo podemos evitarla?

3. Ejercicio 3 (valor: 1/3)

En el ejercicio anterior, el dispositivo IoT emplea un dato R (carga inicial de configuración) que puede ser objeto de algún ataque para descubrirlo, aparte de los ataques de fuerza bruta sobre el protocolo.

Suponga que un atacante adquiere en Internet un dispositivo igual que los nuestros y lo destripa para acceder a sus programas. Luego, logra robarnos uno de los dispositivos con el valor R cargado e intenta extraerlo.

¿Qué opciones tiene para averiguar R?

Describa al menos 2 ataques y la forma de prevenirlos o, al menos, mitigarlos.