VÍDEO intypedia010es

LECCIÓN 10: ATAQUES AL PROTOCOLO SSL

EJERCICIOS

AUTOR: D. Luciano Bello y Dr. Alfonso Muñoz

R&D Security Researcher (Chalmers University)
R&D Security Researcher. T>SIC Group – UPM

EJERCICIO 1

El protocolo SSL es seguro:

a) Siempre. Utiliza tecnología de clave pública que no puede ser invertida

b) Depende de su implementación y configuración

c) Sólo si la herramienta sslstrip se utiliza con la opción -h

d) Si se utilizan certificados X.509v3

EJERCICIO 2

Qué indica el candado amarillo en la url de un navegador web cuando nos conectamos a una página web:

a) Qué la página web es segura

b) Qué se está utilizando el protocolo SSL

c) Qué se está utilizando el protocolo SSL si en la url se adjunta el prefijo https

d) Que el servidor al que nos conectamos es el que nosotros esperamos

EJERCICIO 3

En que afecta funciones aleatorias débiles en la criptografía del protocolo SSL

a) Disminuye el número de servidores al que nos podemos conectar de forma segura
b) En nada si utilizamos algoritmos de clave pública de 1024 bits
c) En que los algoritmos son un poco menos seguros
d) facilita invertir los procesos criptográficos (descifrar comunicaciones y falsificar identidad)

EJERCICIO 4

En qué consiste el ataque NULL byte a certificados digitales:

a) Consiste en enviar cientos de bytes a NULL al cliente para que no identifique los certificados del servidor
b) Reduce a la mitad el tiempo para falsificar un certificado X.509v3
c) Se aprovecha de un tratamiento indebido del campo CN (Common name) de los certificados digitales para falsificar dominios existentes.
d) Debilita la firma digital de los certificados

EJERCICIO 5

Cuál es uno de los mecanismos automáticos recomendados para detectar certificados fraudulentos

a) Verificar a mano la firma digital del certificado
b) Utilizar el protocolo OCSP para analizar el número de serie del certificado. Si esta comprobación no es posible el certificado se debe considerar inválido
c) Los certificados fraudulentos tienen un número de serie que siguen la serie de Fibonacci
d) Ninguno. Dado que no es posible falsificar certificados digitales

RESPUESTAS

1. b
2. c
3. d
4. c
5. b

Madrid, España, Septiembre de 2011

http://www.intypedia.com

http://twitter.com/intypedia