ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
CCPG1003 – INFORMATION ASSURANCE AND SECURITY
TERCERA EVALUACIÓN - II TÉRMINO 2016-2017/ Marzo 3, 2017

Nombre: _____ ***Matrícula:*** _____

COMPROMISO DE HONOR: Al firmar este compromiso, reconozco que el presente examen está diseñado para ser resuelto de manera individual, que puedo usar un lápiz o esferográfico; que sólo puedo comunicarme con la persona responsable de la recepción del examen; y, cualquier instrumento de comunicación que hubiere traído, debo apagarlo y depositarlo en la parte anterior del aula, junto con algún otro material que se encuentre acompañándolo. Además, no debo usar calculadora alguna, consultar libros, notas, ni apuntes adicionales a los que se entreguen en esta evaluación. Los temas debo desarrollarlos de manera ordenada.
Firmo el presente compromiso, como constancia de haber leído y aceptado la declaración anterior. "Como estudiante de ESPOL me comprometo a combatir la mediocridad y actuar con honestidad, por eso no copio ni dejo copiar".

_____
Firma

Tiempo de duración: 2 horas

Tema 1 (30 puntos)

Seleccione una sola respuesta a las siguientes preguntas:

1. ¿Qué algoritmo de clave asimétrica se utiliza para generar de forma segura secretos comunes en los protocolos de seguridad de red más utilizados?
    a. DES
    b. AES
    c. Bin packing
    d. Diffie-Hellman

2. ¿Para calcular el valor hash para un bloque de datos usando una función hash criptográfica como SHA-3 requiere saber la clave secreta correcta?
    a. Sí
    b. No

3. En el ámbito de la seguridad informática, ¿cuál de las siguientes combinaciones define mejor el riesgo?
    a. Amenaza junto con una violación de la seguridad
    b. Vulnerabilidad junto con un ataque
    c. Amenaza junto con una vulnerabilidad
    d. Amenaza acompañada de una violación

4. ¿Incluso si existiera el hardware para realizar todas las operaciones de criptografía casi inmediatamente, la búsqueda de una determinada URL a través de HTTPS todavía tomará un poco más de tiempo de lo que sería utilizando HTTP normal?
    a. Sí
    b. No

5. ¿Qué es lo contrario a C.I.A. en la gestión de riesgos?
    a. Autorización, no repudio, integridad
    b. Mal uso, exposición, destrucción
    c. Divulgación, alteración, destrucción
    d. Confidencialidad, integridad, disponibilidad

Tema 2 (35 puntos)

Conteste a las siguientes preguntas y *justifique en máximo 5 líneas* sus respuestas.

Compártelo! es un popular servicio que permite a los usuarios almacenar archivos "en la nube". Para cualquier archivo que un usuario desea compartir, el usuario carga el archivo (a través de su navegador) a Compártelo! y recibe una URL que proporciona acceso directo al archivo. Cada URL tiene el formato https://Compártelo.com/storage/user/hash, donde *user* es el nombre del usuario que cargó el archivo, y *hash* es el valor hash SHA-256 (64 dígitos hexadecimales) del contenido del archivo. Por ejemplo, una URL podría ser https://Compártelo.com/storage/Alice/9b65...e7e6.

Los usuarios pueden compartir estas URL con sus amigos o con quienes quiera permitir el acceso a los archivos.

(A) (25 puntos) Describa un ataque a la privacidad del usuario que este diseño permite. En su descripción, explique quién podría intentar lanzar el ataque. Realice tan pocas hipótesis sobre las capacidades del atacante como le sea posible.

(B) (10 puntos) Describa una manera que Compártelo! puede defenderse contra este ataque. Su defensa debe requerir cambios mínimos y no interrumpir el modelo de servicio de permitir a los usuarios compartir archivos con amigos.

Tema 3 (35 puntos)

Conteste a las siguientes preguntas y *justifique en máximo 5 líneas* sus respuestas.

Considere un sitio web de comercio electrónico que incluye la funcionalidad de un "carrito de compras". Los clientes que visitan este sitio ponen artículos de interés en su carrito de compras. Después de terminar de elegir los artículos, utilizan el botón de *Checkout* para pagar por ellos. En ese momento, el cliente se identifica en el sitio (con su usuario y contraseña) para permitir que el sitio recupere su información de pago.

(A) (10 puntos) Supongamos que el sitio implementa el carrito de compras almacenando los datos asociados con los artículos y precios en archivos en el servidor, con un archivo para cada cliente. El sitio identifica a los clientes por sus direcciones IP.

Este diseño es vulnerable a un ataque DoS. Explíquelo en *una sola oración*.

(B) (25 puntos) Supongamos que ahora el sitio mantiene una lista de artículos del carrito de compras en el lado del cliente. Cada vez que un usuario hace click en *add-to-cart*, el servidor envía todos los detalles asociados con el artículo (nombre del artículo, precio, cantidad) en su respuesta, incorporándolos en un campo oculto del formulario HTML. A través de la magia de Javascript, ahora cuando el usuario finalmente hace click en *Checkout*, todos los artículos previamente comprados, almacenados en el campo oculto del formulario oculto, se envían al servidor. El servidor los une en una lista y presenta al usuario el valor total correspondiente para el pago.

1. ¿Es este diseño vulnerable al ataque de DoS que ha descrito arriba? Explique su respuesta.

2. ¿Es este diseño seguro contra otros ataques? Si es así, explique su respuesta. Si no es seguro, describa un ataque contra este nuevo diseño. (Puede suponer que el sitio no es vulnerable a ataques web como buffer overflow, CSRF, XSS, inyección de SQL, etc. y utiliza HTTPS para el procedimiento de compra.)