ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
CCPG1003 – INFORMATION ASSURANCE AND SECURITY
TERCERA EVALUACIÓN - I TÉRMINO 2017-2018/ Septiembre 15, 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 (15 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. ¿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

Tema 2 (10 puntos)

Las máquinas virtuales y sandboxes son dos mecanismos utilizados para aislar entidades y lograr confinamiento. Explique *en máximo 5 líneas* el problema de seguridad que estos mecanismos están resolviendo.

Tema 2 (25 puntos)

A y B quieren establecer un canal de comunicación seguro entre ellos. No les importa la confidencialidad de los mensajes que se transmiten, pero sí quieren garantizar la integridad y autenticidad de los mensajes. Responda las siguientes preguntas dibujando diagramas que muestren los procedimientos de envío y recepción de mensajes. Supongamos que A y B comparten una clave común K.

(A) (10 puntos) ¿Cómo pueden lograr su objetivo usando solo criptografía de clave secreta? Si necesita modificar o extender las premisas originales, deberá indicar el cambio en su respuesta.

(B) (10 puntos) ¿Cómo pueden lograr su objetivo usando únicamente una función hash?

(C) (5 puntos) ¿Pueden obtener no repudio? (2 puntos) En caso afirmativo, ¿cómo? Si no, ¿por qué? (3 puntos)

Tema 3 (50 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 el menor número de 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.