


Criterios de evaluación y condiciones de entrega

- Para cualquier duda y/o aclaración sobre el enunciado tenéis que dirigiros al consultor responsable de vuestra aula.
- Se tiene que entregar la solución en un archivo en formato PDF. 
- El nombre del archivo tiene que ser **ApellidoNombre_asignatura_PEC3** con extensión **.pdf**
- Razonad la respuesta en todos los ejercicios e indicad todos los pasos que habéis realizado para obtener la solución.
- Las respuestas sin justificación, que sean una copia de una fuente de información y/o que no contengan las referencias utilizadas, no recibirán ninguna puntuación.
- La fecha límite de entrega será el día **21 de diciembre de 2019** antes de las **23:59h**. La entrega se realizará a través del REC (*Registro de Evaluación Continuada*).

Enunciado

Después de leer los módulos de *Seguridad en servicios de voz sobre IP y mensajería instantánea* y de *Redes emergentes. MANET, WSN, DTN*, resolved cada uno de los siguientes ejercicios y responded a las preguntas que se os formulan.

Ejercicio 1 (3 puntos)

Sin lugar a dudas los servicios de mensajería han emergido en los últimos años, haciendo que cada vez tengan más usuarios. Algunos de estos servicios –como los muy utilizados WhatsApp, Signal y Telegram– proveen incluso de cifrado extremo a extremo para preservar la privacidad de sus usuarios. A pesar de esto, el cifrado extremo a extremo no siempre es una garantía. Recientemente, se han publicado algunas vulnerabilidades de los servicios de mensajería de Whatsapp y Signal. En las siguientes URL tenéis más detalles sobre estas vulnerabilidades:

<https://www.securityweek.com/signal-rushes-patch-serious-eavesdropping-vulnerability>
<https://gbhackers.com/whatsapp-vulnerability/>

Después de leerlos atentamente estos artículos, responded a las siguientes preguntas para cada una de las vulnerabilidades:

- ¿Qué permite la vulnerabilidad a un atacante?
- ¿Quién puede explotar esta vulnerabilidad?
- Explicad con más detalle en qué consiste la vulnerabilidad.
- ¿Qué importancia tiene la Ingeniería Social para poder llevar a cabo el ataque?
- ¿Está solucionada actualmente la vulnerabilidad? ¿Cómo/Por qué?

Ejercicio 2 (3 puntos)

Los servicios de *car sharing* son muy útiles para minimizar el impacto ecológico derivado del uso del vehículo privado. Sin embargo, estos servicios suelen estar controlados de una manera centralizada y requieren el uso de dispositivos móviles conectados a una red de telecomunicaciones, lo que tiene un gran impacto en la privacidad de los usuarios.

Para contar con las ventajas del *car sharing* y preservar al mismo tiempo la privacidad de los usuarios, se propone una solución basada en la distribución del control mediante el uso de una red oportunista de tipo DTN y el uso del cifrado homomórfico.

Tanto conductores como pasajeros enviarán sus ofertas y peticiones, respectivamente, de manera oportunista (directamente de dispositivo a dispositivo, utilizando un protocolo de encaminamiento oportunista como P_{Ro}PHET).

Contesta y razona las siguientes cuestiones referidas a este escenario:

- ¿Podrían utilizarse en esta red los protocolos de encaminamiento de redes Ad Hoc, como AODV o OLSR? Justifica tu respuesta.
- Si se quiere garantizar el secreto y la autenticidad de las comunicaciones, razona si es mejor utilizar en este caso un esquema basado en el establecimiento de claves a partir de una clave maestra de corto plazo, o un esquema de IBC.
- En qué consiste el cifrado homomórfico? ¿Para qué crees que podría utilizarse en este caso? Pista: los conductores escogen al pasajero que esté dispuesto a pagar más, siempre que lleguen a un precio mínimo, pero no necesitan saber el importe justo hasta que la persona sube al vehículo.

Ejercicio 3 (4 puntos)

Este último ejercicio consiste en un cuestionario *online* que tenéis que responder. Este cuestionario hace referencia a los módulos 5 y 6 de la asignatura. Para acceder al cuestionario tenéis que ir al enlace “Cuestionarios” del aula y entrar en el correspondiente a la PEC 3. Es importante que tengáis en cuenta:

- Es muy recomendable que hayáis repasado los módulos antes de iniciar el test.
- Tenéis dos intentos para hacer el test. La nota final será la nota más alta de los dos intentos.
- La duración del test es de un máximo de 30 minutos por cada intento.
- El test se puede realizar hasta la fecha de entrega de la PEC 3.