Departamento de Lenguajes y Sistemas Informáticos
E.T.S. Ingeniería Informática. Universidad de Sevilla

Avda Reina Mercedes s/n. 41012 Sevilla
E-mail lsi@lsi.us.es **Web** www.lsi.us.es

E.T.S. ingeniería informática

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

CAI 1. CONSULTA SOBRE CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE CONTRASEÑAS (Parte 2)

La entidad bancaria permite a sus clientes realizar transferencias financieras a través de la aplicación para móviles que pueden descargar. Para mantener la integridad de las transferencias, la transmisión se hace de **"forma segura"** usando **Códigos de Autenticación de Mensajes (MAC)** para los mensajes realizados por el cliente al servidor con **claves secretas de tamaño 32 bits.** Dicha entidad entrega a los clientes cada año un dispositivo físico (pendrive, smartcard, SD memory, …) que contiene dicha clave para realizar todas las gestiones financieras que deseen durante el año. No obstante, el Equipo de Gobierno que nos ha contratado, tiene dudas razonables sobre la robustez del algoritmo de generación de MAC y las claves usadas para los MAC por dicha aplicación para dispositivos móviles.

La **Política de Seguridad propuesta por el Gobierno de la Seguridad de la Información (SI)** de la entidad bancaria especifica **que todas las transmisiones de información de la entidad con los clientes deben ser íntegras,** evitando **los posibles ataques de man-in-the-middle y replay.**

Las consultas que nos hace el cliente son las siguientes:

a. ¿Es seguro el tamaño de clave que estamos usando para la integridad de las transmisiones? Dado el siguiente mensaje y su correspondiente MAC enviados entre el cliente de la entidad bancaria, compruebe **el tiempo mínimo que se tardaría en encontrar la clave, muestre el proceso a seguir y la clave obtenida, y cuál es de media el tiempo que se tarda en descubrir la clave**. **Razone si es un tiempo lo suficientemente alto como para garantizar la seguridad de la clave.** Para ello utilice los siguientes mensajes de diferentes clientes (diferente clave) y su correspondiente MAC:

Mensaje	MAC
`531456_487654_200`	`c5173b3e13fbed7f1b41c7dfa5fd6fd6368cd366`
`541157_487655_200`	`158413dd62eada5273a72f9fa35f4e19ddb864b8`
`541158_487656_200`	`0a5f910eddc60e3b06f51670e83d37886804bf9a`

Los mensajes tienen la estructura: **CuentaOrigen_CuentaDestino_Cantidad**. (20%)

b. **En caso de que no considere que la clave es robusta, debería indicar el tamaño exacto de clave** que sería conveniente (**48 bits ?, 64 bits ? 128 bits ? …)**. Presente en el informe los criterios que ha considerado para llevar a cabo la selección del tamaño de clave adecuado, **justificando detalladamente** su elección. El cliente nos comunica que valora muy positivamente **TODAS LAS PRUEBAS EMPÍRICAS QUE SE APORTEN PARA AVALAR TAL JUSTIFICACIÓN.** (15%)
c. Se debe detallar el procedimiento a llevar a cabo para **que el cliente y servidor tengan la misma clave para hacer la comprobación de la integridad.** Proponer una política

adecuada para la entrega de las claves a los clientes, informando del procedimiento que se deba seguir, las personas y/o sistemas implicados, y la periodicidad. Detalle como el banco debe custodiar las claves hasta que sean entregadas, como será el proceso de entrega, y en que soporte se le entregará la clave. Tenga en cuenta la información que el banco conoce de sus clientes para asegurar que el proceso sea lo más seguro posible. (15%)

Normas del entregable

- Cada ***Security Team X*** debe entregar el informe ST-X-CAI1B.pdf que contenga todos los detalles que responden a los puntos de la consultoría (se debe indicar expresamente los alumnos del equipo que han participado en el trabajo) a través de la actividad creada al efecto en el curso de Enseñanza Virtual. El informe debe recoger evidencias del proceso, herramientas y pruebas realizadas, así como de las respuestas a las consultas planteadas.
- La consulta se desarrollará en la sesión dispuesta al efecto, y en el tiempo indicado por el profesor.