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 2. CONSULTA SOBRE LA INTEGRIDAD DE LA TRANSMISIONES DE UNA ENTIDAD BANCARIA CON APP

Nuestro cliente es en este caso una entidad bancaria que 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.**

La entidad bancaria entrega a los clientes cada año un dispositivo físico (*pendrive, smartcard*, …) que contiene dicha clave para realizar todas las transferencias financieras que deseen durante el año. No obstante, el Equipo de Gobierno SI, 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. (Valoración 20%).** 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**.

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. (Valoración 15%)**

c. **Desplegar un verificador de integridad en los sistemas cliente/servidor para llevar a cabo la realización de la verificación de forma práctica de los mensajes transmitidos entre un servidor y un cliente. (Valoración 35%).** Se debe tener en cuenta que:
   - **Como entrada se recibirá el mensaje (Cuenta Origen, Cuenta Destino, Cantidad)** a verificar la integridad en su transmisión, y se debe poder especificar el nombre del **algoritmo** que se usará para verificar la integridad, y la **clave utilizada por el cliente y el servidor** para cada cuenta bancaria origen.
   - **Output del sistema:** Indicación en el cliente y servidor si se ha conservado la integridad o no se ha conservado. La salida podría ser presentada en una ventana al emisor del mensaje y en el servidor dejar constancia en **un fichero de logs de los mensajes que no han llegado de forma íntegra y de la ratio de mensajes que se envían de forma íntegra/número total de mensajes enviados entre los usuarios y la entidad financiera**

d. Explique las medidas de seguridad tomadas para evitar problemas de incumplimiento de la Política de Seguridad relacionada con la **integridad de las transmisiones** usando el algoritmo de MAC. Por ejemplo, para evitar **posibles ataques de man-in-the-middle, replay o similares. (Valoración 15%)**

e. 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. (Valoración 15%).** 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, y en que soporte se le entregarán. Tenga en cuenta la información que el banco conoce de sus clientes para asegurar que el proceso sea lo más seguro posible.

El cliente no tiene preferencia alguna por el desarrollo del cliente/servidor en cualquier lenguaje de programación. No obstante, la entidad financiera nos ha facilitado la tarea a llevar a cabo enviándonos parte del desarrollo servidor y cliente, para que la solución se base en sockects.

Normas del entregable

- El plazo de entrega de esta consultoría finalizará el próximo **día 11 de noviembre a las 8.30 horas.**
- Debe entregar el informe EquipoXCAI2.pdf que contenga todos los detalles que responden a los puntos de la consultoría y un zip con el proyecto (se debe indicar expresamente los alumnos del equipo que han participado en el trabajo).