INGENIERÍA DE SEGURIDAD US
E.T.S. Ingeniería Informática. Universidad de Sevilla
Avda. Reina Mercedes s/n. 41012 Sevilla
Tlf/Fax 954 557 139 **E-mail** lsi@lsi.us.es **Web** www.lsi.us.es

PAI 1. INTEGRIDOS - VERIFICADORES DE INTEGRIDAD EN EL ALMACENAMIENTO Y TRANSMISIÓN PARA ENTIDAD FINANCIERA

Introducción

En este **Proyecto de Aseguramiento de la Información** usaremos técnicas para poder verificar **la integridad en el almacenamiento y la transmisión de datos por redes públicas como Internet y evitar los diferentes tipos de posibles ataques, concretamente los de Man-in-the-Middle, Replay, Key derivation y de canal lateral de tiempo.**

En este caso, una entidad financiera desea ofrecer servicios de transferencia a sus clientes usando una arquitectura cliente-servidor como la del esquema de la Figura 1.

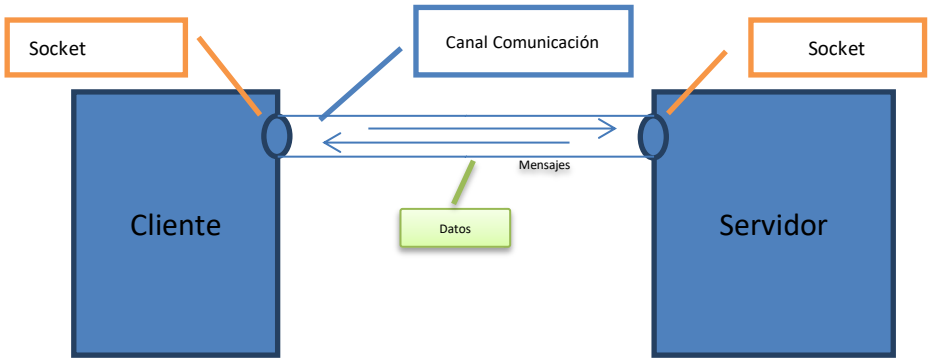

Figura 1: Arquitectura de la entidad financiera

La entidad nos plantea que usará un mecanismo de credenciales (nombre de usuario y contraseña) para identificar a los clientes para poder comprobar qué usuarios pueden conectarse a dicha entidad. La entidad financiera contará con un sistema de registro de usuarios simplificado de tal manera que el usuario solo necesite indicar un nombre de usuario y una contraseña para su registro. Además, la entidad financiera contará de partida con varios usuarios dados de alta en su aplicación y que podrán conectarse al servidor. El sistema servidor de la entidad financiera dispondrá de un mecanismo de autenticación que permita a los usuarios introducir sus credenciales y en la parte servidora un mecanismo para verificar dichas credenciales. Tras comprobar sus credenciales, se mantendrá abierta la sesión en la que se le ofrecerá al usuario la opción de cerrar la sesión o realizar transacciones (una o varias) con el siguiente formato:

"***Cuenta origen, Cuenta destino, Cantidad transferida***"

Dichas transacciones no tendrán que pasar ningún tipo de validación de cuentas y cantidades previa y serán registradas en el servidor sin más comprobación.

Política de Seguridad

La entidad financiera tiene definido las siguientes **Políticas de Seguridad**, que indica lo siguiente referente a las transacciones y el almacenamiento de información:

*"Se debe preservar la **integridad en el almacenamiento de credenciales de usuario**"*

"**En todas las transacciones **por medios electrónicos no seguros se debe conservar la integridad** de las comunicaciones**"

Por lo tanto, el servidor de la entidad debe asegurar la integridad de la información de la información de los usuarios registrados, y conectados y además de las transacciones realizadas.

Objetivos del proyecto

A continuación, se propone a los equipos de trabajo los siguientes objetivos:

1. Desarrollar un sistema cliente-servidor usando sockets, que permita enviar datos de nombre de usuarios, contraseñas, y mensajes de transacciones cumpliendo los aspectos indicados en la Política de Seguridad de la empresa.
2. Desarrollar en el servidor un mecanismo que permita registrar, almacenar y comprobar las credenciales de usuario preservando la integridad de la información.
3. Desarrollar el verificador de integridad para los mensajes de transferencia bancaria que se transmiten a través de las redes públicas, evitando los ataques de *man-in-the-middle,* de *replay (tanto en el servidor como en el cliente), de key derivation, de canal lateral*, usando mecanismos de MAC, NONCE, TAMAÑOS DE CLAVE ADECUADOS y SECURE-COMPARATOR.
4. Analice y discuta las diferentes opciones que existen para la compartición segura de claves y cuál sería más adecuado para evitar incidentes de seguridad.

Recomendaciones para el desarrollo

Arquitectura

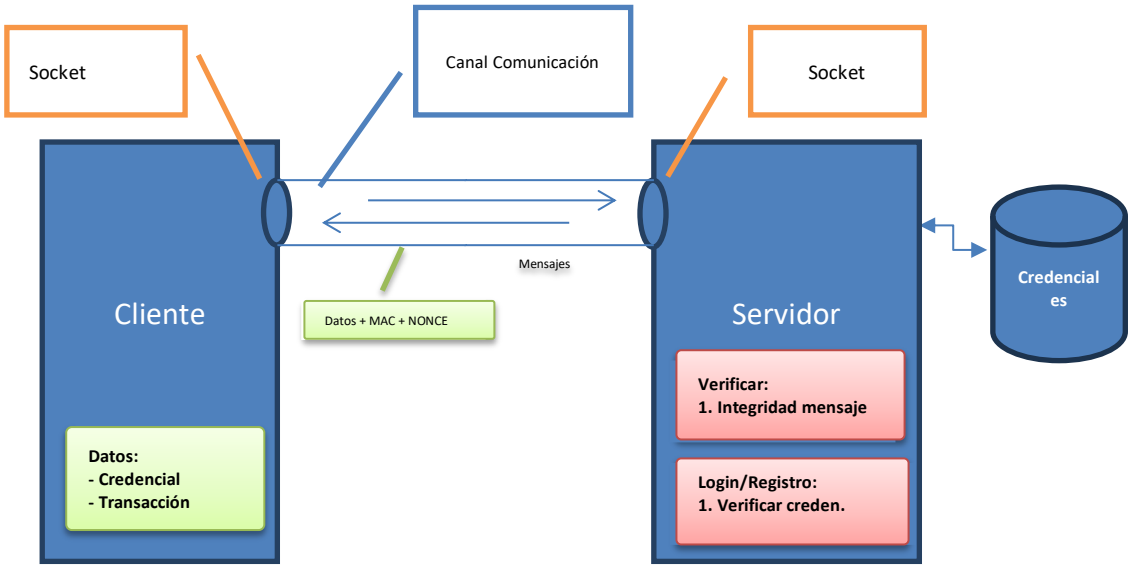

Figura 2: Arquitectura propuesta para la entidad financiera

Requisitos funcionales

1. **Registro de usuarios:**

    - Permitir que un nuevo usuario se registre proporcionando únicamente un nombre de usuario y una contraseña.
    - Informar al usuario si ya existe un registro con el mismo nombre de usuario.
    - No permitir modificaciones a los datos de usuarios después del registro.

2. **Inicio de sesión:**

    - Permitir a los usuarios registrados iniciar sesión introduciendo su nombre de usuario y contraseña.

3. **Verificar credenciales:**

    - Validar las credenciales proporcionadas contra los datos almacenados en el servidor.
    - Denegar acceso si las credenciales no coinciden con un registro válido.

4. **Cerrar sesión:**

    - Permitir a los usuarios ya logados cerrar la sesión.

5. **Gestión de usuarios preexistentes:**

    - El sistema debe contar con un conjunto inicial de usuarios registrados para que puedan acceder sin necesidad de registrarse.

6. **Transacciones:**

    - Permitir a los usuarios autenticados realizar transacciones en el formato, no se debe validar cuentas o cantidades:
        - **"Cuenta origen, Cuenta destino, Cantidad transferida".**

7. **Persistencia de datos:**

    - Registrar y almacenar de manera permanente:
        - Los datos de los usuarios.

8. **Interfaz de comunicación:**

    - Proveer una interfaz (usando sockets) que permita a los clientes interactuar con el sistema de registro, autenticación, y transacciones.

Requisitos de Información

El sistema debe poder almacenar información relacionada con:

1. **Datos de usuarios:**
    - Cada usuario debe tener:

        - Nombre de usuario (único).
        - Contraseña.
2. **Registro inicial:**
    - El sistema debe contar con una base de datos inicial con:
        - Una lista de usuarios pre-registrados.
        - Sin transacciones realizadas previamente.

El sistema debe gestionar la siguiente información:

3. **Transacciones:**
    - Cada transacción debe incluir:
        - Cuenta origen (identificador).
        - Cuenta destino (identificador).
        - Cantidad transferida (valor numérico).
4. **Mensajes del sistema:**
    - Informar al usuario en las siguientes situaciones:
        - Usuario registrado exitosamente.
        - Usuario ya registrado.
        - Inicio de sesión exitoso o fallido.
        - Transferencia realizada con integridad

Requisitos de seguridad

1. **Requisitos de Seguridad para las Credenciales de Usuario**
    - Almacenamiento Seguro de Credenciales
    - Verificación Segura de Credenciales
    - Protección Contra Ataques en Login (BruteForce)
2. **Requisitos de Seguridad para las Transacciones**
    - Integridad en la Comunicación de Transacciones
3. **3. Requisitos de Seguridad para la Base de Datos**
    - Integridad de los datos almacenados en base de datos.

La recomendación para la implementación de la verificación de la integridad en la transmisión de mensajes es usar el siguiente esquema que se muestra en la Figura 3.

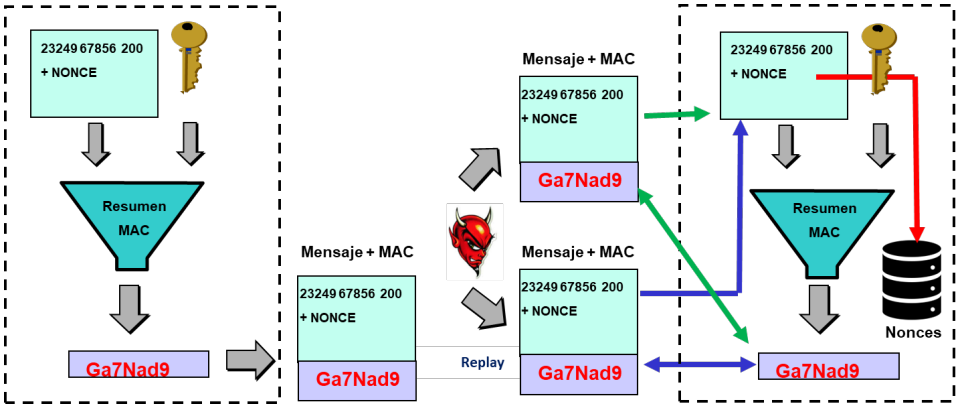

Figura 3: Esquema ejemplo de verificación de integridad de mensajes.

Consideraciones

- El sistema de almacenamiento puede ser cualquier tipo de base de datos que permita almacenar la información, pero debe tener en cuenta la seguridad que ofrecen cada una de las soluciones de almacenamiento propuestas.
- Se puede utilizar cualquier lenguaje de programación.
- Se deben utilizar sockets para la comunicación, y ***no es necesario implementar un protocolo seguro.***

Normas del entregable

- Cada Security Team debe entregar a través de la Plataforma de Enseñanza Virtual y en la **actividad** preparada para ello un archivo zip, nombrado ***PAI1-STX*.zip**, que deberá contener al menos los ficheros siguientes:
  - ✓ **Informe en formato PDF que contenga un informe/resumen del proyecto** con los detalles más importantes de las decisiones, soluciones adoptadas y/o implementaciones desarrolladas, así como el resultado y análisis de las pruebas realizadas (máximo 10 páginas).
  - ✓ **Código fuente de las posibles implementaciones o scripts desarrollados o configuraciones establecidas en herramientas, así como los archivos de las pruebas desarrolladas, archivos de logs y/o evidencias oportunas**
- El plazo de entrega de dicho proyecto finaliza el **día 7 de octubre a las 23:59 horas.**
- **Los proyectos entregados fuera del plazo establecidos serán considerados inadecuados por el cliente y por tanto entrarán en penalización por cada día de retraso entrega de 10% del total, hasta agotarse los puntos.**
- **El cliente no aceptará envíos realizados por email, ni mensajes internos de la enseñanza virtual, ni correo interno de la enseñanza virtual. Toda entrega realizada por estos medios conllevará una penalización en la entrega del 10%.**