Universidad de los Andes
Ingeniería de Sistemas y Computación
ISIS 2203 Infraestructura Computacional

Caso de Estudio 2 – Canales Seguros
Logística y Seguridad Aeroportuaria

Objetivos

- Identificar los requerimientos de seguridad de los canales usados para transmisión de la información en el sistema de Logística y Seguridad Aeroportuaria.
- Construir un prototipo a escala del sistema que permita satisfacer algunos de los requerimientos de seguridad identificados. Entendiendo las garantías de seguridad y las limitaciones de la implementación propuesta.

Problemática:

Como se indicó en el enunciado del caso, el sistema cuenta con varias aplicaciones: Novasoft financiero en línea y fuera de línea, OpenERP, Sistema Time & Attendance, correo electrónico y página web. En este contexto, surgen diversos problemas de seguridad para algunas de las transacciones que el sistema soporta, tanto a nivel de transmisión, como en procesamiento y almacenaje de datos. Como consecuencia, es necesario evaluar riesgos y determinar medidas para mitigar los problemas detectados.

Su tarea en este caso es actuar como consultor de seguridad y analizar, considerando solo aspectos de seguridad, las tareas relacionadas con la aplicación Time & Attendance.

Tareas:

Suponga que el sistema tiene tres servidores, uno soporta la aplicación financiera, el segundo soporta el sistema time & attendance y correo electrónico y el tercero soporta la página web.

- Los servidores uno y dos manejan control de acceso a nivel del sistema operativo y ejecutan transacciones solo para usuarios autorizados. Las aplicaciones también manejan usuarios y ejecutan transacciones solo para usuarios autorizados. El tercer servidor no requiere autenticación, solo presenta información de interés general para sus clientes, empleados y socios. Y no almacena documentos con requerimientos de confidencialidad.

A. [20%] Análisis y Entendimiento del Problema.

En el sistema descrito en el párrafo anterior:

1. Identifique y describa cinco amenazas al sistema descrito en los párrafos anteriores. Explique su respuesta en cada caso (*) y responda la pregunta ¿Si la amenaza se consolida, cómo afectaría al sistema?
2. Identifique cinco vulnerabilidades del sistema, teniendo en cuenta únicamente aspectos técnicos (no organizacionales o de procesos). Identifique vulnerabilidades no solo en lo relacionado con la comunicación sino también con el almacenamiento y procesamiento de los datos. Explique su respuesta en cada caso (*).

(*) *Sus explicaciones DEBEN estar ligadas al contexto del problema planteado e indicar cómo. NO se aceptarán respuestas para contextos genéricos.*

B. [10%] Propuesta de Soluciones.

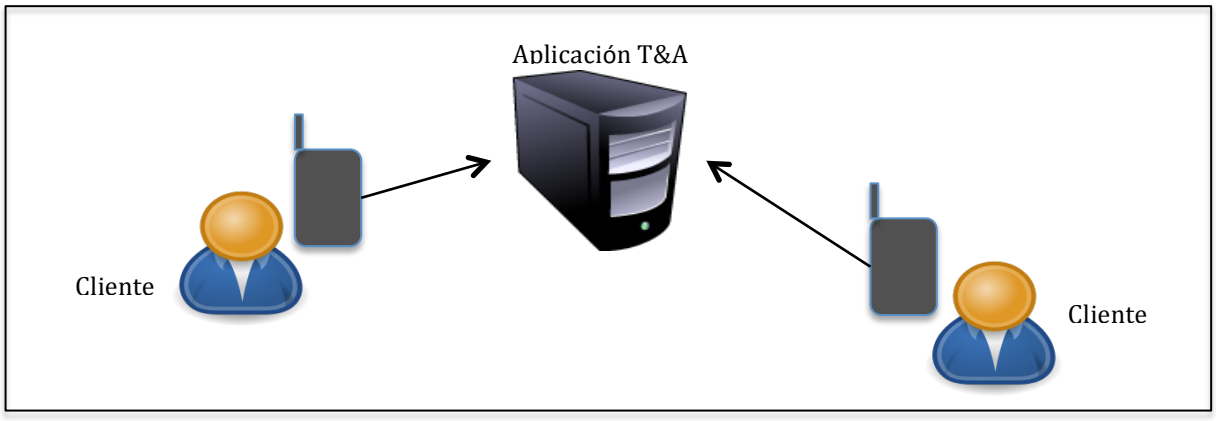
Para cada una de las amenazas que usted identificó en el punto anterior, proponga mecanismos de resolución/mitigación.

- Los mecanismos propuestos deben ser explicados, por ejemplo, si se habla de cifrado sobre un canal de comunicaciones, debe identificar los participantes en la comunicación, y si es cifrado simétrico o asimétrico (y justificar la decisión).
- Además, debe justificar los mecanismos propuestos. Es decir, identifique explícitamente cuál riesgo mitiga y cómo.

En sus justificaciones tenga en cuenta aspectos relacionados con eficacia, costo, eficiencia, flexibilidad, aspectos de implementación, y otros aspectos técnicos que considere convenientes.

C. [70%] Implementación del Prototipo.

En esta parte del proyecto nos centraremos únicamente en la aplicación de Time & Attendance.



Su tarea consiste en construir un cliente que se comunique con el servidor para reportar una posición y la hora de llegada.

El agente y el servidor seguirán el protocolo descrito a continuación para su comunicación:

1. El agente se comunica con el servidor para iniciar una sesión de actualización de posición, y espera un mensaje de confirmación.
2. El agente envía la lista de algoritmos de cifrado que usará durante la sesión y espera un mensaje del servidor confirmando que soporta los algoritmos seleccionados (si no, el servidor envía un mensaje de terminación).
3. El agente envía su certificado digital (CD) para autenticarse con el servidor. El CD debe seguir el estándar X509.
4. El servidor verifica el certificado digital del agente y envía su propio certificado digital (CD) para autenticarse con el agente. El CD debe seguir el estándar X509.
5. El servidor genera una llave simétrica (LS) y la envía al agente. Para proteger la llave, el servidor usa la llave pública del agente (KC+).
6. El agente recibe la llave protegida y la extrae.
7. El agente genera un mensaje de confirmación, cifrando la misma llave simétrica, con la llave pública del servidor.
8. A continuación el agente usa la llave simétrica para cifrar la información de posición y envía el código de integridad correspondiente.
9. El servidor recibe la información y chequea integridad. Si no hay problemas la almacena. Después envía respuesta al cliente, OK o ERROR, anunciado el resultado de la comunicación y la terminación de la comunicación.

La figura 1 ilustra el protocolo.

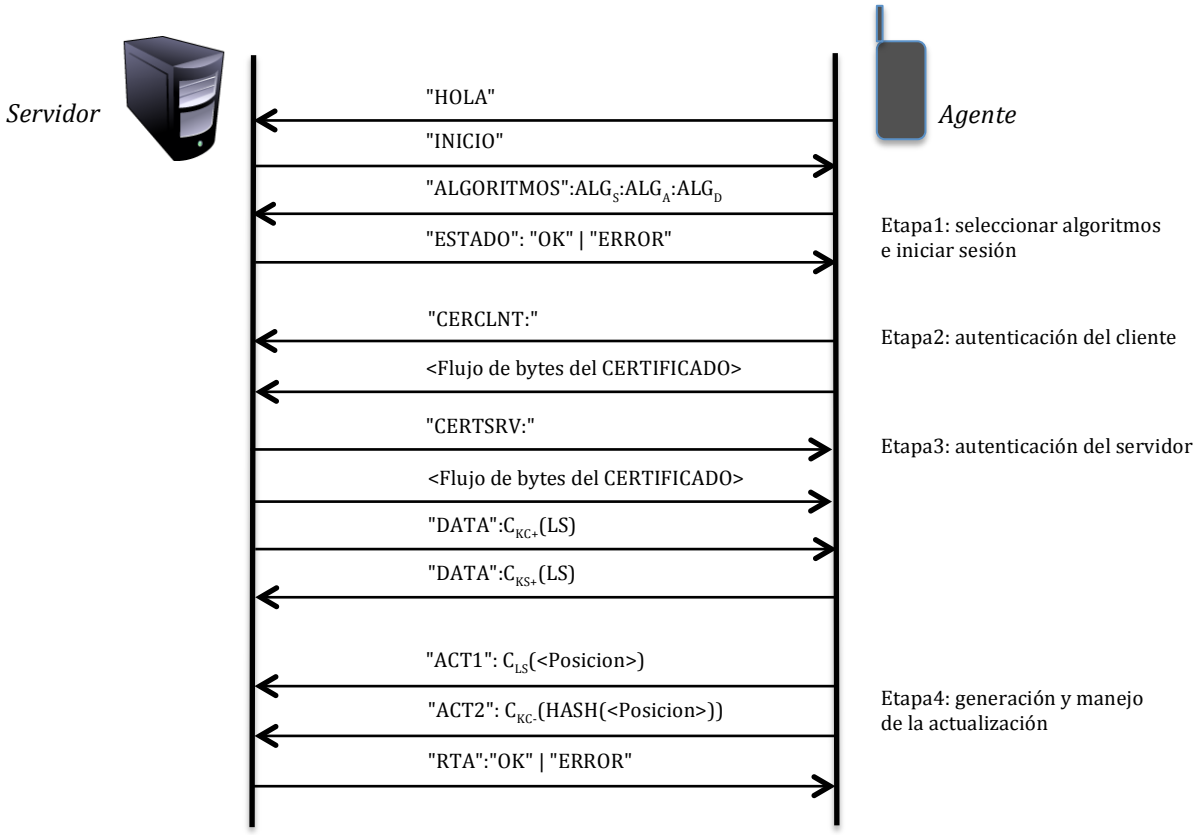


Figura 1. Protocolo de comunicación entre agente y servidor.

PARA TENER EN CUENTA:

- El protocolo de comunicación maneja la siguiente convención:
  - Cadenas de Control: "HOLA", "INICIO", "ALGORITMOS", "ESTADO", "OK", "ERROR", "CERTSRV", "CERTCLNT", etc.
  - Separador Principal: " : "
- A continuación se presentan los algoritmos disponibles en el servidor para manejo de las tareas de cifrado. Es decir, los algoritmos que deben reemplazar las cadenas ALG_S, ALG_A y ALG_D en el protocolo. Para implementar el cliente usted debe seleccionar un algoritmo en cada caso.
  - Simétricos (ALG_S):
    - DES. Modo ECB, esquema de relleno PKCS5, llave de 64 bits.
    - AES. Modo ECB, esquema de relleno PKCS5, llave de 128 bits.
    - Blowfish. Cifrado por bloques, llave de 128 bits.
    - RC4. Cifrado por flujo, llave de 128 bits.
  - Asimétricos (ALG_A):
    - RSA. Cifrado por bloques, llave de 1024 bits.
  - HMAC (ALG_D):
    - HmacMD5
    - HmacSHA1
    - HmacSHA256

  Las cadenas que identifican cada uno de los algoritmos son: "DES", "AES", "Blowfish", "RC4", "RSA", "HMACMD5", "HMACSHA1", "HMACSHA256".
- Utilizaremos la versión 3 del estándar X509 para el CD. La idea es que el agente puede comprobar la identidad del servidor a partir de un CD (en un caso real este debería ser expedido por una entidad certificadora pero aquí se va a generar localmente). El CD debe seguir el estándar X509, en particular, debe contener la llave pública para usarla en el proceso de comunicación (puede usar la librería Bouncycastle para la generación del certificado). El agente también se autentica con un certificado digital.

- La posición se manejará como dos parejas de números (grados y minutos en decimal), separados por una coma ",". Por ejemplo: 41 24.2028, 2 10.4418 (coordenadas usadas por Google).
- La comunicación se realiza a través de sockets de acuerdo con el protocolo de comunicación definido.
- El código de envío del certificado debe lucir como se indica abajo. Es decir, primero se indica que se enviará el certificado y luego se envía el contenido (en bytes).

```
writer.println( CERTIFICADO );
java.security.cert.X509Certificate cert = certificado( );
byte[] mybyte = cert.getEncoded( );
socket.getOutputStream( ).write( mybyte );
socket.getOutputStream( ).flush( );
```

- Dado que existen problemas en la transmisión de los bytes cifrados, se manejará encapsulamiento con cadenas hexadecimales para transmisión de enteros.
- Se entregará una versión del servidor para que puedan realizar pruebas.
- Habrá una versión sin seguridad para hacer pruebas del protocolo. La figura 2 ilustra el protocolo sin seguridad.

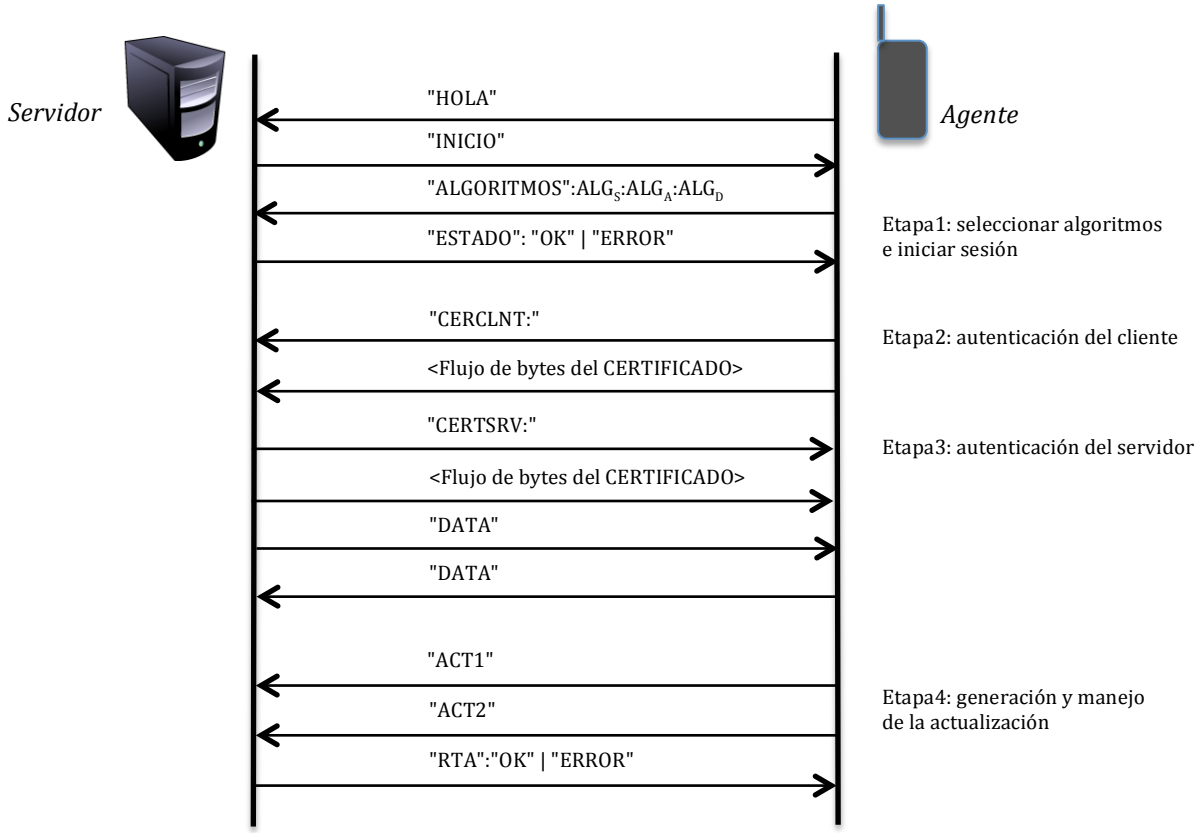


Figura 2. Protocolo sin seguridad.

Entrega:

Cada grupo debe entregar un archivo zip que incluya el informe (con las respuestas a las tareas A y B) y un proyecto Java con la implementación correspondiente al agente (descrito en la parte C). El informe vale 30% y la implementación 70% de la calificación del caso 2.

Referencias:

- *Cryptography and network security*, W. Stallings, Ed. Prentice Hall, 2003.
- *Computer Networks*. Andrew S. Tanenbaum. Cuarta edición. Prentice Hall 2003, Caps 7, 8.
- *Blowfish*. Página oficial es: http://www.schneier.com/blowfish.html
- *RSA*. Puede encontrar más información en: http://www.rsa.com/rsalabs/node.asp?id=2125
- *CD X509*. Puede encontrar la especificación en: http://tools.ietf.org/rfc/rfc5280.txt
- *MD5*. Puede encontrar la especificación en : http://www.ietf.org/rfc/rfc1321.txt