

**Infraestructura computacional**

**Ingeniería de Sistemas y Computación**

**ISIS-2203**

Daniela Mariño - 201412576

Joan Torres - 201315711

María Arévalo - 201415326

**Caso de Estudio 2 - Canales Seguros**

**Logística y Seguridad Aeroportuaria**

1. **Análisis y entendimiento del problema**
2. **Amenazas detectadas en la aplicación Novasoft financiero en línea**

* **Modificación no autorizada de datos**

Actualmente, el intercambio de información no tiene un mecanismo que verifique la integridad de los datos recibidos. Este problema, ligado con el hecho de que el mensaje no viene cifrado, permite que un atacante pueda interferir en la comunicación, modificar el mensaje y enviarlo de nuevo sin problema. Si esta amenaza se cumpliera aumentaría la generación de errores y la integridad de los datos guardados en la base de datos se vería afectada.

* **Robo de información**

Debido a que la información enviada entre el cliente y el servidor de Novasoft no está cifrada, personas externas podrían tener acceso a ella más fácilmente. Y, al ser información sensible, esta podría ser explotada para realizar ataques a futuro a la aplicación o a sus clientes (aeropuertos, aerolíneas, servicios terrestres, entre otros).

* **Suplantación de identidad**

Al no haber un sistema de autenticación de fuente/destino en la transmisión de datos e.g. certificado digital, un atacante puede decir ser el cliente (transportista, aeropuerto, aerolínea, etc) o el servidor Novasoft y obtener o modificar información de esta manera. Si esta acción se consolida, una persona no deseada podría enviar datos erróneos tanto al servidor como al cliente, afectando la integridad de estos.

* **Acceso no autorizado al sistema**

Se sabe que cada aplicación maneja su propio archivo de usuarios, pero no se tiene información de la seguridad de dicho archivo o de la seguridad de sus datos. Si, por ejemplo, el sistema maneja un sistema de autenticación básico (contraseñas cortas sin restricciones) algún agente externo podría intentar hacerse con dichas contraseñas por fuerza bruta. Si alguien no autorizado entrara al sistema, se podría dar un robo de información, una suplantación de identidad o una modificación no autorizada de datos directamente en la base de datos.

* **Desastre natural en Colombia**

Actualmente Novasoft solo puede ser accedido desde las sedes de “Logística y Seguridad Aeroportuaria S.A.” en Colombia. Si ocurriera un desastre natural en este país, o un problema de electricidad, la empresa no tendría como acceder a toda su información financiera.

1. **Vulnerabilidades del sistema**

* **Sincronización de datos de Novasoft al final del día**

Debido a que algunas sedes internacionales usan la aplicación Novasoft financiero fuera de línea durante el día y esperan hasta cierta hora para sincronizarse con Novasoft financiero en línea, la aplicación podría no aguantar la cantidad de usuarios y colapsar. Novasoft en línea es una aplicación que está al límite de sus capacidades, una cantidad de información muy grande podría llevar a un buffer overflow que sobre escribiría información importante de la base de datos.

* **Falta de autenticación fuente/destino en envío de datos**

A pesar de que se tiene una autenticación local del usuario, no hay garantía de que el destinatario de los datos sea el servidor de Novasoft. Por otro lado, siendo receptor de los datos, no se puede garantizar que el emisor sea el cliente que dice ser.

* **Envío de datos no cifrado**

Actualmente, el envío de datos al servidor de Novasoft se hace sin cifrado, por lo que hace más fácilmente para otra persona espiar la información que es enviada. Ni el servidor ni el cliente manejan llaves públicas o privadas, por lo que no se garantiza el no-repudio. Para la empresa, esta es una vulnerabilidad crítica, ya que se manejan datos de aeropuertos, aerolíneas y empresas de carga que son sensibles, y podrían tener graves consecuencias si caen en malas manos.

* **Falta de mecanismo de verificación de integridad de datos**

Como fue mencionado anteriormente, la aplicación carece de autenticación fuente/destino, y esto lleva a que la información que se envía sea modificada sin que ninguna de las dos partes se dé por enterada. Novasoft no tiene un mecanismo que contrarreste esta situación, como lo podría ser una función digest, lo que hace más fácil al atacante modificar la información.

* **Almacenamiento de datos sin cifrado**

Los datos manejados por la aplicación son de contabilidad, tesorería, cuentas, facturación, etc… Como en cualquier empresa, estos son sensibles, y actualmente Novasoft no tiene ningún mecanismo donde se especifique que se guarden cifrados, lo que hace más fácil a un ser externo o interno tener acceso a ellos.

1. **Propuesta de soluciones**

A continuación, se presentan mecanismos de mitigación para las amenazas identificadas anteriormente:

* **Modificación no autorizada de datos**

Mecanismo de mitigación: Implementación de función de hash

Para garantizar la integridad de los datos enviados, el cliente enviará el mensaje cifrado con la llave simétrica, así como la función de hash aplicada al mismo mensaje, cifrado con la llave simétrica. El Servidor debe descifrar el mensaje, así como la función de hash, y después aplicar la función de hash acordada anteriormente al mensaje obtenido. Finalmente, al comparar estas dos funciones de hash y obtener lo mismo se garantiza la integridad de datos. Si son iguales, el servidor envía un OK con la respuesta a la consulta, de lo contrario envía el mensaje de error.

* **Robo de información**

Mecanismo de mitigación: Sobre digital y llave de sesión.

Una vez obtenidas las llaves públicas de cada parte mediante el CD, se envía dentro de un sobre digital (cifrado asimétrico) la llave simétrica a utilizar en la transacción (llave de sesión). Para poder obtener esta llave, se tiene que decodificar con la llave privada de cada parte. Esta acción, complementa la mitigación de la amenaza de suplantación de identidad. Una vez obtenida la llave simétrica, todas las consultas después de este punto estarán cifradas con ella. Se tomó la decisión de usar cifrado asimétrico una vez y después simétrico debido a que el asimétrico es más costoso en cuanto a recursos, y el simétrico es más eficiente. Entonces, se garantiza mayor seguridad en la parte crítica, la cual es establecer comunicación por primera vez, y una vez validado este paso se continúa con cifrado simétrico.

* **Suplantación de identidad**

Mecanismo de mitigación: Certificado Digital.

Para mitigar esta amenaza, se propone que el cliente antes de enviar información sensible, envíe su certificado digital (generado por una EC), donde garantice su identidad. Así mismo, el servidor central debe responder con el su certificado digital para que el cliente esté seguro de que se está comunicando con el servidor. En este intercambio, se envían las llaves públicas y se tiene una estampilla cronológica para garantizar que no se ha vencido. Se usará el estándar X509 para generar este certificado.

* **Acceso no autorizado al sistema**

Mecanismo de mitigación: Endurecimiento de máquinas.

Con el fin de mitigar esta amenaza se propone a la empresa minimizar los permisos actuales de los usuarios, así como tener diferentes niveles de defensa para que el archivo de configuración no pueda ser alterado. También, se sugiere actualizar estos datos cada cierto tiempo, para evitar que los ataques de fuerza bruta sean efectivos.

* **Desastre natural en Colombia**

Mecanismo de mitigación: Cambiar implementación

Tener acceso a una aplicación desde un solo lugar puede ser perjudicial para la empresa, por eso nuestro mecanismo de mitigación es el de cambiar la implementación de la aplicación y dejar que sedes de otros países también puedan acceder a ella. Si se protege la información y se maneja bien la autenticación y autorización de los usuarios, este cambio de implementación no debería generar problema.