

**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**

* **Acceso no autorizado al sistema**

Cada aplicación del sistema maneja su propio archivo de configuración de usuarios, donde se define lo que pueden o no hacer. Sin embargo, no es explícito la forma en que este es guardado y quien tiene acceso a él. Al ser un archivo estático sin protección alguna, un atacante externo puede tener acceso a él y robar las credenciales de un cliente autorizado. Por otro lado, al interior de los aeropuertos se podría presentar que el atacante se auto conceda más privilegios, por ejemplo, una guardia podría atribuirse derechos de tesorería. Si esto se consolida, se podrían dar ataques internos a la aplicación (instalación de software malicioso), y no se garantizaría el no-repudio. Además de que agentes externos obtengan información confidencial y la puedan manipular a su conveniencia.

* **Modificación no autorizada de datos**

Actualmente, el intercambio de información no tiene un mecanismo que verifique la integridad de estos. Ligado con el hecho de que estos no vienen cifrados, el atacante puede interferir en la comunicación y modificarlos. Si esto sucede, se tendrán datos erróneos guardados en las bases de datos, los motivadores de negocio de Novasoft se ven fuertemente afectados, ya que no se tendrá un margen de ganancia verídico y aumentará la generación de errores.

* **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. Al ser información de operaciones de aeropuertos, esta podría ser explotada para realizar ataques a futuro a la aplicación, además del hecho de que son datos confidenciales de aeropuertos, aerolíneas, servicios terrestres y carga.

* **Suplantación de identidad**

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

* **Fraude**

Debido a que Novasoft internacional utiliza la aplicación fuera de línea, y hace una sincronización diaria de sus datos, al no ser esta en tiempo real, un atacante puede ser aparentemente dos personas al mismo tiempo. Por ejemplo, una aerolínea que opera tanto a nivel internacional como nacional podría registrar una compra en ambas aplicaciones al tiempo, ya que no están sincronizadas, y al final del día, Novasoft no sabría cual información es verdadera.

1. **Vulnerabilidades del sistema**

* **Sincronización de datos de Novasoft fuera de línea al final del día.** Debido a que al final del día Novasoft financiero fuera de línea envía los datos obtenidos de la jornada, se pueden presentar problemas con respecto a la consistencia de esos datos. Al sincronizar las bases de datos simultáneamente de las 17 sedes internacionales, no se tiene claro la estampilla cronológica de las transacciones y no se puede garantizar la consistencia 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:

* **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.

* **Robo de información**

Mecanismo de mitigación: Cifrado con llaves públicas y privadas.

Una vez obtenidas las llaves públicas de cada parte mediante el CD, se envía mediante un cifrado asimétrico la llave simétrica a utilizar en la transacción. 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.

* **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.

* **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.

* **Fraude**

Mecanismo de mitigación: Implementar Novasoft en línea en sedes internacionales.

Con respecto a esta amenaza, se propone que a nivel internacional se gestione independientemente su contabilidad, pero que tan pronto sea procesada y almacenada localmente, esta sea enviada inmediatamente a la sede principal de Novasoft. Esto implica implementar la versión en línea de Novasoft, haciendo que la sincronización de los datos sea en tiempo real, garantizando la integridad de datos y que los usuarios no puedan hacer 2 o más transacciones sobre la misma aplicación al tiempo.