Gabriel Pinto Pineda - 201515275
Santiago Saenz Gonzalez - 201512416

Caso 2

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

PARTE 1

En nuestro grupo de proyecto, logramos identificar diferentes datos que deben ser protegidos, entre estos se encuentran los siguientes a enumerar, que posteriormente serán explicados:

a) El certificado digital del servidor
b) El certificado digital del cliente
c) La llave simétrica
d) Las coordenadas

Explicación

a) El certificado digital del servidor

El certificado digital es la forma en la que se puede comprobar que una conexión es básicamente seguro. Un certificado digital, para ser considerado como fiable, debe estar asociada a una entidad certificadora. En nuestro caso no hay ninguna entidad asociada por lo que mantener el certificado encriptado es esencial para poder evitar fallas de seguridad en la cual se pueda utilizar el mismo certificado por otra entidad, podría conllevar a un caso de *spoofing.*

Respuesta:

En caso de que un ente no autorizado obtenga la información del certificado podría suplantar al servidor lo cual permitiría el envío de información del cliente a una entidad que no está autorizada para recibir información y que generaría *Information disclosure*, lo que comprometería las coordenadas de los vehículos y por ende podría comprometer la operación completa.

b) El certificado digital del cliente

El certificado digital del Cliente es primordial, como se había planteado en el anterior caso del certificado del Servidor, es primordial para mantener una conexión seguro.

Se debe proteger este certificado ya que permitiría generar un caso de *spoofing* en el cual se permitiría generar un caso de *tampering*.

Respuesta:

En el caso de un tercero acceda a la información del certificado de un cliente podría suplantar a un verdadero cliente para mandar información de incorrecta al Servidor, simplemente para poder confundir a los coordinadores. Por otro lado, el caso de *tampering* podría complicarse aún más ya que podría hacer inyecciones a las base de datos que podrían comprometerla no solo para los datos que envíe el supuesto servidor del cliente, sino con la información de los otros clientes verídicos, que han enviado información.

c) **La llave simétrica**

La llave simétrica debe ser protegida puesto que es con ella que se cifra la información relacionada con la ubicación de las unidades de distribución. Si un actor externo la obtiene, sería capaz de conocer el mecanismo por el cual son cifradas las coordenadas, incrementando así el riesgo de que estas sean descifradas.

Respuesta:

En el caso en el cual un acto no permitido sea capaz de obtener acceso a esta llave, en el caso de lectura, podría ser capaz de descifrar la posición de las unidades de distribución, incurriendo en los riesgos mencionados en el literal “d”. En el caso de escritura, podría ser capaz de modificar dicha llave, por lo que es posible que los actores con acceso no sean capaces de descifrar las coordenadas de posición al tener una llave diferente, generando así un incorrecto funcionamiento del sistema.

d) **Las coordenadas**

Este dato debe ser protegido dentro del sistema de rastreo ya que indica en tiempo real la posición que tienen las unidades de distribución. Y si un actor accede a esta información, podría afectar significativamente a la empresa.

Respuesta:

Si un actor no autorizado logra tener acceso a las coordenadas de posición, en el caso de la lectura, lograría saber la ubicación exacta en tiempo real de las unidades de distribución y en un escenario pesimista, podría interceptar y robar el contenido de este. En el caso de escritura, sería capaz de modificar dicha ubicación, por lo

que no sería posible conocer a ciencia cierta dónde se encuentra la unidad de distribución perdiendo así correcto seguimiento de este y exponiéndose a posibles problemas.

PARTE 2

En el caso del protocolo dado anteriormente, existen diferentes vulnerabilidades que pueden permitir casos de *Spoofing* , *Tampering* e *Information Disclosure,* por diferentes razones.

Vulnerabilidad 1

En una primera instancia, los certificados usados en el proceso de comunicación entre el servidor de posición y las unidades de distribución, son certificados que no tiene una entidad certificadora asociada (o por lo menos una que verificada y autorizada). Esta situación implica entonces que no hay una certeza de que el certificado que es enviado por la unidad de distribución, y aquel que es enviado por el SP sean realmente certificados verificado y con alta confiabilidad, por esto, podría tratarse de un caso de spoofing.

Vulnerabilidad 2

En una segunda instancia, existe una vulnerabilidad subsecuente con la transmisión de datos que existe entre el servidor de posición y las unidades de distribución, ya que podría darse la situación en que el cliente, sea capaz de mandar una inyección de sql (asumiendo de que hay una base de datos) o de mandar datos tipo malware, lo cual podría afectar la información que se está almacenando sobre las unidades de distribución u otra información de suma importancia.

Vulnerabilidad 3

En una tercera instancia, existe el riesgo de que las unidades de distribución sean suplantadas por otra entidad y generen certificados que el servidor considere como válidos, obteniendo así la capacidad de elevar sus privilegios y acceder a datos no permitidos como lo es la llave simétrica y el certificado del servidor.

Vulnerabilidad 4

Por ultima instancia, todas las operaciones son procesadas por un mismo y único servidor. Al ser una unidad física, y como todo componente de hardware, el servidor es proclive a presentar algún tipo de falla en el procesamiento de las peticiones o

incluso en su funcionamiento. Adicional a esto, es posible que se realice una gran cantidad de peticiones a la vez que pueden hacer inhabilitar al servidor y su capacidad de respuesta, y por otra parte, es más sencillo para los actores hacerle seguimiento a un único servidor con el fin de cometer actos no permitidos.

B. [10%] Propuesta de Soluciones.

Vulnerabilidad 1

Mecanismos:

El mecanismo primordial que se debe utilizar es el de la encriptación *RSA.* Este tipo de encriptación es asimétrico, el cual alivia el problema de pasar las claves a través de Internet, pero es más lento y requiere más potencia de procesamiento en las computadoras tanto del remitente como del destinatario para cifrar y descifrar los mensajes. Las claves públicas pueden ser distribuidas libremente, pero una clave privada es conservada por un usuario y nunca es compartida.

Justificación:

Debido a que el certificado, como ya habíamos mencionado, es esencial para evitar casos de *spoofing* y de *tampering*, fue necesario considerar algún tipo de algoritmo de encriptación que fuese lo suficientemente seguro para poder mantener esta información a salvo. En el caso de del *RSA,* este nos asegura que las vulnerabilidades que pueden generar los casos de infracción de seguridad sean mitigado, básicamente por dos razones:

a) No se necesita canales seguros para mandar la clave. La distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario.

b) No hay desbordamiento en el tratamiento de claves y canales.

Vulnerabilidad 2

Mecanismos:

El primer paso a tener en cuenta para tener un mecanismo es el uso debido de los certificados, esto implica hacer las autenticaciones necesarias para que se valide que el servidor y el cliente sean legítimos, lo cual implicaría que un caso de

tampering podría ser descartado. Por otro lado, en el caso en que por alguna extraña razón se haya suplantado al cliente, debe existir una autenticación por parte del servidor que permita asegurarse de que lo enviado por parte del cliente sea meramente una encriptación de las coordenadas. Para esto se envía la llave con la que se pretende encriptar el código y se espera que se envíe las coordenadas encriptadas con una función hash que asegure que es el código que se pretende.

Justificación:

El uso de certificadores es la forma más confiable de generar una conexión segura. Por otro lado, la función hash permite asegurar la integridad y veracidad de los datos por varias razones. La primera es que proporciona integridad de datos y protección contra manipulación indebida de una manera similar a las firmas digitales, pero no requiere que las partes que se comunican tengan claves públicas y privadas ,y la segunda es que los HMAC también proporcionan un mejor rendimiento para las comunicaciones masivas en línea que las tecnologías de firma digital de clave pública. Estos elementos son fundamentale para que se pueda combatir la segunda vulnerabilidad.

Vulnerabilidad 3

Mecanismos:

Con el fin de mitigar esta vulnerabilidad se deberían implementar un sistema de autenticación y autorización adicional basado en los tokens de sesión. Cada una de las unidades de distribución debería primero acceder al sistema con credenciales válidas, que a su vez deben estar protegidas, las cuales son verificadas por otro servicio implementado dentro del servidor para este proceso y después de esto si continuar con el procedimiento descrito.

Justificación:

Al tener un sistema de autorización y autenticación, el servidor se asegura que las peticiones/respuestas que se están llevando a cabo, son con un cliente (unidad de distribución) autorizada y validado por el sistema, por lo que reduce el riesgo de enviar su certificado y llave simétrica en una gran medida a posibles actores sin permisos. Adicionalmente, al acceder con credenciales verificadas y validadas, se puede asumir que el certificado enviado por el cliente (en caso de ser aceptado) posee de un cliente con permisos para realizar dicha tarea.

Este mecanismo incrementa la eficacia del proceso ya que solo se limita a trabajar con clientes autorizados, sin embargo, reduce la eficiencia al tener que implementar la verificación de las credenciales enviadas.

Vulnerabilidad 4

Mecanismos:

Con el fin de prevenir la pérdida de capacidad de respuesta debido a problemas que puede presentar el unico servidor de posición, causando consigo problemas sobre el estado de los paquetes y afectando directamente a la compañía es posible implementar un servidor adicional. El servidor adicional recibiría peticiones enviadas por las unidades de distribución a su vez, reduciendo la carga de un único servidor, y siendo soporte en caso de que alguno de los 2 presente fallos.

Por otra parte, con este servidor se podría implementar un nuevo mecanismo de seguridad en el cual el cliente dirija la petición a uno de los 2 servidores y este se encargue de verificar si dicho cliente se encuentra en la lista de clientes que tienen el derecho a comunicarse con el.

Justificación:

Tener más de un servidor de posición permite que las peticiones sean respondidas de una forma más eficaz y adicionalmente permite que en caso de que uno de los 2 servidores falle, el sistema no quede completamente desconectado. A partir de dicho planteamiento, se mejora la eficacia y la usabilidad, sin embargo, se aumentan a su vez los costos implicados con la compra y mantenimiento del servidor.

Adicional a esto, se justifica que el servidor permitiría la repartición de clientes por atender y dicha repartición sería algo que se mantendría de carácter confidencial en la unidad de almacenamiento del servidor, por lo que si el servidor recibe la petición de un cliente no permitido, el sistema podría reconocer que se trata de una amenaza a la seguridad e integridad del sistema, incrementando con esto la seguridad.