Ingeniería de Sistemas y Computación

Infraestructura Computacional

María Paula Mancipe Díaz

Santiago Abisambra Castillo

Abril 10, 2015

**Caso 2**

**Seguridad**

Amenazas

1. Si una persona hurta una unidad de distribución, tiene acceso al itinerario entregas de ese día y si no se puede desactivar la comunicación entre ésta y el servidor, es probable que el ladrón tenga la oportunidad de conocer el itinerario de entregas, enviando información incorrecta hacia el sistema de rastreo.

Si esto ocurriera, la empresa pensaría que ya se han entregado varios pedidos por la información que envió el ladrón y no tendrían forma de responder a las quejas de los clientes porque no hay un registro de esa unidad que no haya sido intervenido por el ladrón.

1. Se podría modificar la información que pasa a través del canal de comunicación entre el sistema de rastreo y el sistema de paquetes para crear rutas, de modo que se asignen unas rutas distintas a las unidades de distribución.

Si esto ocurre, se podría direccionar las unidades hacia puntos en la ciudad donde personas roben las encomiendas para entregar y obtengan acceso desde las unidades hacia el sistema, para seguir hurtando información.

1. Si el servidor es atacado y el componente de procesamiento es afectado, se podría almacenar información errónea que no brinde las estadísticas correctas para el funcionamiento de la empresa.

Si esto ocurre, probablemente, la empresa tome decisiones incorrectas que vayan en detrimento de ella, sin saber lo que está ocurriendo.

1. El protocolo de comunicación podría ser modificado de modo que las unidades de distribución no se puedan comunicar con el sistema y se queden esperando una respuesta de este.

Si esto ocurre, la unidad no podrá informar cada 60 s lo que esté ocurriendo con las entregas.

1. El canal de comunicación entre las Unidades de Distribución con el sistema podría ser re direccionado hacia otro servidor en el cual se almacene toda la información de las entregas y la estrategia que utilizan en la empresa para realizarlas. Si esto ocurre, la información podría ser vendida a la competencia o filtrada al público.

Vulnerabilidades

1. Puesto que no hay cifrado en la mensajería, alguien podría hacerse en el medio del canal de comunicación entre el sistema de rastreo y las unidades de distribución, solo para escuchar la información que transmite la UD cada 60s.

Si esto ocurriese, la persona que esté interviniendo en la comunicación, podría vender esa información o tener un cómplice que esté en el momento en el que una unidad este distribuyendo un paquete.

1. El servidor podría ser atacado con muchos requerimientos falsos de Unidades de Distribución ficticias, colapsando el sistema de rastreo y no permitiendo atender los requerimientos de las Unidades de Distribución reales.

Si esto ocurriese, toda la empresa podría verse afectada porque las unidades de distribución no podría reportar su ubicación ni sus entregas realizadas. Por lo tanto, la empresa podría entrar en caos y asignar status erróneos a las entregas.

1. Otro servidor podría suplantar el servidor que tiene el sistema de rastreo y procesar la información de la unidad de distribución para crear datos falsos que pongan en peligro la información del destinatario.

Si esto ocurre, se estaría enviando información errónea a las unidades, de modo que no podrían hacer la entrega correcta.

1. Dentro del servidor, alguien podría suplantar el administrador de la base de datos que se encarga de persistir la información, almacenando información errónea y más información de la debida.

Si esto ocurre, se perdería la información en tiempo real de la entregas. Es decir que si un remitente tiene un reclamo, no habría forma de consultar los registros con información veraz.

1. Si el servidor es atacado, la información persistida en el sistema de rastreo no está cifrada. Esa información estaría disponible al mejor postor y podría ser filtrada en Internet.

Si esto ocurriese, la competencia podría conocer detalles de las entregas y crear una mejor estrategia de ventas

Soluciones

1. Para proteger la información en el canal de comunicación se podría utilizar cifrado asimétrico desde el sistema de rastreo hacia la unidad de distribución y viceversa. A pesar de que esta solución afectaría el desempeño del sistema, permitiría a ambas partes cifrar la información con una llave pública, pero solo la parte interesada tiene la llave privada para descifrar la información.
2. Para evitar que se creen requerimientos falsos que colapsen el sistema de rastreo, tanto la unidad de distribución como el servidor del sistema de rastreo deberían tener certificados digitales que se puedan validar y que cambien cada dos semanas. Este último argumento se debe a que se está enviando cada 60 s una gran cantidad de información, en 15 días hay un volumen considerable de información que está siendo enviada o requerida del servidor.
3. La información que procese y envié el servidor debería estar cifrado con la llave publica de cliente. Además de esto, se podría generar un código criptográfico de hash que me permita verificar la veracidad de la información que está siendo enviada.
4. Para saber que esa información fue persistida en óptimas condiciones. La información debería ser almacenada con el código criptográfico de hash, de modo que cuando se haga una petición de la información, se compare la información almacenada que sea procesada con la función contra el código ya almacenado.
5. Para evitar que la información sea filtrada o vendida fácilmente, se puede tomar un atributo clave del cual dependa el resto de información de cada entrega y se cifra con una llave simétrica. A pesar de que esto afecte el desempeño de la aplicación, haría más difícil que la información pueda ser obtenida con facilidad.