**UNIVERSIDAD DE LOS ANDES**

**INFRACOMP**

**CASO 2 - SEGURIDAD**

Juliana Montes Maestre 201111355

Johnathan Nimoy 201214989

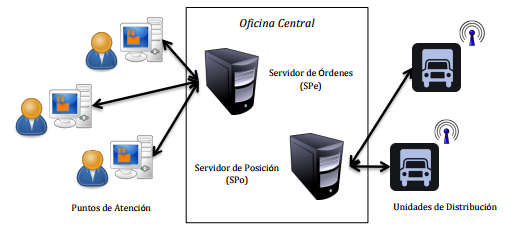
1. Identifique y describa los datos que deben ser protegidos en el sistema de manejo de órdenes. Explique su respuesta en cada caso(\*) y responda la pregunta ¿Si un actor no autorizado consigue acceso al dato mencionado, ya sea en modo lectura o escritura, cómo podría afectar la empresa?

* Debe ser protegida la información personal de los clientes, en la cual se guarda su información de facturación, dirección, etc. En caso de que un autor acceda a ella en modo lectura podría emplear la información para transacciones a crédito que maneja el usuario y usarlas para hacer compras a su nombre y robarlo, por medio de suplantación, o conocer su teléfono y dirección para un posible robo o chantaje.
* Debe ser protegida la información de envío en los paquetes. Si un externo logra acceder en modo lectura a esta información podría rastrear el paquete e interceptarlo, o si accede en modo escritura podría afectar la integridad de esta información para que el envío sea dirigido a otro, ya sea porque este otro tiene un interés en el paquete o porque se desea evitar que el dueño original lo reciba.
* Debe protegerse la información de estado de las unidades de distribución. En caso de que esta información pueda ser alterada, no se llevaría un registro íntegro de los estados de los pedidos, lo que afectaría la garantía que brinda la empresa distribuidora sobra la información de los paquetes. Adicionalmente se genera un problema de seguridad en cuanto a que se puede perder la capacidad de monitoreo sobre las unidades, y si se planea un ataque armado a una de estas no podría reportarse o prevenirse.

2. Identifique cuatro vulnerabilidades del sistema de manejo de órdenes, 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 corresponder al contexto planteado (de forma explícita). NO se aceptarán respuestas para contextos genéricos.

Vulnerabilidades encontradas:

En el contexto actual, el sistema presenta una serie de vulnerabilidades asociadas a la seguridad en el almacenamiento y transporte de la información desde los puntos de atención al servidor y viceversa. Teniendo en cuenta que se cuenta con la siguiente arquitectura:



Se encuentran las siguientes vulnerabilidades:

1. El servidor de órdenes posee problemas de seguridad en el almacenamiento de datos en la base de datos puesto que no se realiza cifrado sobre dichos registros comprometiendo la confidencialidad y la integridad de la información almacenada.
2. La comunicación entre el servidor y los puntos de atención no presenta ningún tipo de cifrado por lo cual se compromete la confidencialidad de la información en el transporte de información ida y vuelta entre el servidor y los puntos de atención.
3. Se presentan problemas de autenticación puesto que no hay mecanismos que permitan al servidor identificar si el mensaje proviene de un Punto de Atención autorizado o si viene de un tercero, pasa lo mismo con los puntos de atención.
4. Hay una gran vulnerabilidad en el transporte de los mensajes puesto que se envían sin ningún mecanismo de detección de cambios en los mensajes transportados, por lo cual se amenaza la integridad de la misma.

B. [10%] Propuesta de Soluciones. Para cada una de las vulnerabilidades que usted identificó en el punto anterior, proponga mecanismos de resolución. - 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 qué vulnerabilidad resuelve y justifique. En sus justificaciones tenga en cuenta aspectos relacionados con eficacia,

1. Se sugiere la implementación de un mecanismo de cifrado para la persistencia de la información de los paquetes en la base de datos del servidor de órdenes. Así, en caso de que alguien logre acceder a la misma, necesitaría de una llave para poder decifrar la información buscada. Se recomendaría en particular un mecanismo de cifrado asimétrico, que a pesar de ser costoso, da una mayor garantía de seguridad. Para implementar cifrado asimétrico se requerirían dos llaves, una privada y una pública, y en este caso particular se usaría la llave pública para cifrar los datos que van a la base, y la llave privada (que por ser privada sólo la tendrían un grupo específico de usuarios) se usaría para descifrar estos datos al ser retribuídos.
2. Para esta vulnerabilidad se propone implementar un mecanismo de cifrado simétrico, el cual otorga confidencialidad al sistema durante la comunicación. Se manejaría una llave de sesión efímera sería otorgada por el servidor, quién manejaría las sesiones de cada cliente . De esta forma se lograría confidencialidad, pues el intercambio de mensajes sólo se puede dar entre aquellos que conozcan las llaves.
3. A partir del cifrado propuesto en el punto anterior también se estaría implementando autenticación. Esto se debe a que sólo podrían participar de la comunicación quiénes conocen las llaves, y esto genera autenticación a partir de un objeto único que se posee (sólo un grupo selecto las posee).
4. Para verificar la integridad de la información de los paquetes se incorporaría una firma digital. Para la implementación de esta se modificaría la estructura de la información, de tal forma que se divida en dos, y la comparación de estas dos partes permitiría detectar una modificación de la información y tomar las medidas pertinentes. Las dos partes del mensaje consistirán en el mensaje original y el mismo mensaje cifrado usando un algoritmo conocido sólo por las dos partes (e.j. algoritmo de hashing), y para el cifrado por medio de este algoritmo se usaría la llave de sesión.