**Caso 2**

Infraestructura Computacional 201920

María Camila Londoño - 201713578

Carlos Fernando Infante - 201713454

**1. Identifique los datos que maneja el portal web y que deben ser protegidos. 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 a la entidad?**

Los datos que maneja el portal web son la cédula para iniciar sesión y la clave, estos deben estar protegidos de manera que se pueda verificar autenticidad, confidencialidad e integridad. En el portal existe un rol de afiliado y empleado. Este portal es el que permite el acceso a la aplicación del historial laboral, por ende, el proceso que se realiza es el de autenticarse a la plataforma en línea y poder acceder desde ella la aplicación. Según el documento que contextualiza el problema, ‘‘la información más importante que maneja la empresa tiene que ver con personas (afiliados), y con empresas (aportantes), y su relación’’. Entonces es muy grave que un actor no autorizado consiga la clave correspondiente a una cédula, puesto que si no existe confidencialidad de la información, los clientes perderán confianza en la organización y preferirán otra compañía de fondos de pensiones. Si se logra ingresar en modo lectura, se puede obtener todos los datos del afiliado, en el historial laboral se encuentra información sensible de cada usuario incluyendo sus tarjetas del banco, sueldo, empresas en las que se ha trabajado, etc. Teniendo esa información puede haber problemas legales por suplantación, pérdida de dinero al usar las tarjetas, robos, etc. Si se logra acceder en modo escritura, puede existir un problema aún mayor, ya que se pueden modificar datos sensibles generando inconsistencias en la información que contiene cada cliente. Por otro lado, si es una cuenta con rol de administrador se podría redireccionar información, borrar cuentas y modificarlas. Así que si un agente malicioso consigue el acceso a una cuenta en el portal, es perjudicial no solo para el negocio sino también para el cliente de manera directa, el impacto es grande, con las vulnerabilidades descritas en el punto dos, se podrá evidenciar la probabilidad de ocurrencia.

**2. Identifique cuatro vulnerabilidades de este sistema, teniendo en cuenta únicamente aspectos técnicos o de procesos (no organizacionales). 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.**

* La información se encripta según el protocolo planteado con una clave de sesión lo cual es una llave simétrica, esto tiene sus ventajas y desventajas. Al ser llaves simétricas, su proceso de encriptar y desencriptar es más rápido que el de una asimétrica, lo cual es necesario ya que uno de los requerimientos es que el tiempo de respuesta desde cualquier oficina y desde Internet sea menor o igual a 4 segundos. Estas llaves existen por un tiempo limitado lo cual es ideal para este caso de uso, ya que el tiempo promedio que un usuario realiza una actividad en el portal web al ser una consulta dura de minutos a horas. La mayor ventaja de usar llaves de sesión, es el volumen, puesto que al ser únicas las llaves de sesión y la empresa tener en su portal web 1000 transacciones al día y 1.900.000 afiliados en general, el número de llaves a las que un atacante necesita para acceder, es grande. Sin embargo, esto genera varias vulnerabilidades, una es que no es tan complicado para un atacante encontrar el patrón de generación de las llaves, puesto que los algoritmos bajo las cuales estas están hechas, aunque son rápidos, no son tan seguros como los podría ser una llave asimétrica. Este problema de seguridad debe ser disminuido tomando varias medidas, una de ellas es el tiempo de vida de una clave de sesión. Sin embargo, la mayor desventaja es que las sesiones están siendo guardadas en una memoria en el servidor, pero dependen de las cookies las cuales se pueden secuestrar (hijack).
* Otra vulnerabilidad encontrada es la parte del protocolo cuando se hace el envío como cliente del “reto” hacia el servidor porque podrían pasar dos cosas: se envía algún mensaje que es interceptado por alguien que hace Man In the Middle y cambia el reto. Esto podría ser un problema porque puede no ser de longitud múltiplo 4 y puede que al momento de recibir el mensaje encriptado por el servidor no sea el mismo que se envió entonces no funciona así la llave simétrica si esté bien generada.
* Al momento de enviar los mensajes de OK o de ERROR también pueden interceptados para así cambiarlos y que se escriba un error lo que dañaría el protocolo completo. Esto es un problema porque así todo el manejo y la implementación esté bien hecha, esto puede dañar la autenticación por no saber quién es el que realmente envía el mensaje y la integridad de los datos al cambiarlos mientras están en proceso de envío. Por ejemplo, al momento de enviar los algoritmos que se quieren usar hacia el servidor y que el servidor responda con ‘OK’ se pueden interceptar y que el atacante envíe cualquier otra cosa con tal de dañar el protocolo.
* Nosotros decidimos utilizar para el cifrado simétrico el algoritmo de AES, ya que Blowfish es un proceso lento que produce 4 kByte de tabla por instancia en RAM. Esto comparado a AES puede ser implementado de manera eficiente (al menos en hardware) sin RAM o necesidad de laguna pre-computación. Además la tabla de 4 KB es usada para la implementación rápida de software y puede ser compartida entre instancias, cosa que no puede hacer el algoritmo de Blowfish entonces resulta siendo más lento. Sin embargo hay una vulnerabilidad dentro de AES y es que al momento de realizar el algoritmo hay un punto en que se reduce en 2 bits la longitud de la llave. Esto resulta en un problema pues termina siendo de 126 bits y el tiempo de búsqueda por fuerza bruta se reduce en 3 millones de años. Así mismo, cuando se hace la parte de cifrado por bloques el atacante puede usar meet-in-the-middle para encontrar los valores del cifrado y el descifrado intermedio de modo que ya no necesita esperar antes y después del algoritmo para hacer fuerza bruta y encontrar la llave sino que lo puede hacer dentro del proceso y eso resulta en menos tiempo de espera.

Cabe mencionar que elegimos para la parte del HMAC y garantizar la autenticación la opción de HMAC con SHA512 pues este es el que tiene una mayor seguridad por el tamaño del digest que es 512 bits e igualmente cumple con los requerimientos de tiempo que pide el enunciado.