Departamento de Lenguajes y Sistemas Informáticos
E.T.S. Ingeniería Informática. Universidad de Sevilla

Avda Reina Mercedes s/n. 41012 Sevilla
Tlf/Fax 954 557 139 **E-mail** lsi@lsi.us.es **Web** www.lsi.us.es

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

CAI 4. CONSULTA SOBRE LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA ENTIDAD HOSPITALARIA (II)

En trabajos anteriores los clientes finales de una entidad hospitalaria nos han solicitado proyectos para poder responder a requisitos de seguridad relacionados con la ***integridad y confidencialidad*** de la información con ***autenticación*** de los participantes. Continuando con las consultorías de seguridad debido a que se han detectado incidencias en determinadas radiografías, el Hospital desea añadir una firma oculta en cada una de las radiografías que se realicen. En está consultoría se pide valorar la **esteganografía** como técnica para dar una solución a este problema, ya que consiste en la ocultación de la información sobre un objeto (imagen, sonido, video, …). El Hospital nos comunica que se puede usar cualquier herramienta que considere oportuna el equipo Consultor para el estudio que a continuación nos propone. De acuerdo con ello, se pide:

Apartado 1). Estudio del método LSB.

La entidad hospitalaria nos pide un estudio sobre la idoneidad del método LSB para ocultar la firma en las imágenes (preferiblemente bmp o png). Nos expresa **los criterios de decisión** a tener en cuenta en la consultoría **con imágenes donde el tamaño de las firmas a ocultar está entre 128 y 512 caracteres**:

1. **Tamaño:** Tamaño que debe tener la imagen original para que la firma quede oculta (sin tener que aumentar el tamaño de la imagen original).
2. **Confidencialidad:** Imposibilidad de detectar y/o decodificar las firmas añadidas. ¿Qué medidas se pueden tomar para mejorar la confidencialidad? Presente los resultados.
3. **Tiempo de ocultación** y de **recuperación**: Tiempo que se tarda en embeber la firma y el tiempo que se tarda en obtenerlas de la imagen correspondiente.
4. **Robustez:** representa la cantidad de distorsiones que el estego objeto (imagen) puede soportar antes que se pierda la información oculta y no se perciba que existe texto embebido en el estego objeto. Se podrían probar diferentes distorsiones, como por ejemplo introducir 5 órdenes de distorsión para Salt-Pepper o distorsión Crop para cuatro anchos y altos (W/H) diferentes. ¿Qué se puede hacer para mejorar los resultados ante cada una de las distorsiones aplicadas?

Por todo ello esta **tarea exige experimentación**. Realizar un estudio donde quede reflejado **TODO EL TRABAJO QUE HA REALIZADO** y presentar las pruebas realizadas en los pasos anteriores. **(Valoración 20%)**

Apartado 2). Propuesta de otro método alternativo a LSB.

La entidad hospitalaria nos pide que valoremos de forma análoga al apartado anterior, otro método para ocultar la firma en las **imágenes (puede ser un formato diferente a bmp o png).**

Para los tres primeros criterios anteriores muestre los resultados y compare con LSB para ver cuál es mejor. Realizar un estudio donde quede reflejado **TODO EL TRABAJO QUE HA REALIZADO.** Presentar las pruebas realizadas. Puede utilizar **una herramienta diferente a la del apartado anterior. (Valoración 15%)**

CONSULTA SOBRE LA SEGURIDAD DE LOS CLIENTES WEB

Continuando con las consultorías de seguridad que tienen planteados esta entidad en sus respectivos **Planes Director de la Seguridad de la Información**, se pretende abordar en esta consultoría para mejorar la seguridad de los Clientes Web de su Hospital cuando realizan compras y transacciones.

Estas compras seguras se hacen generalmente a través del protocolo ***https***, que se apoya en el protocolo ***SSL/TLS***. El funcionamiento de dicho protocolo establece que un cliente cuando accede a un servidor mediante dicho protocolo, deben ambos negociar los parámetros de la conexión antes de establecerla. Entre éstos se debe negociar lo que se conoce como "*cipher suite*". El navegador (cliente Web) que se utilice debería contener una lista de versiones del protocolo y algoritmos de cifrado/integridad más seguros y en un orden de seguridad decreciente. Y para ello se hace necesaria la correspondiente modificación de la configuración de los navegadores de los clientes.

Además las últimas vulnerabilidades detectadas con respecto al protocolo SSL/TLS han permitido extraer datos de conexiones seguras. La vulnerabilidad que se conoce como POODLE (***Padding Oracle On Downgraded Legacy Encryption***) es un ataque de man-in-the-middle donde es posible descrifrar un mensaje cifrado usando SSL v3.0. Por tanto es muy importante evitar el compromiso del cifrado. También habría que evitar las más recientes (FREAK, LOGJAM, SLOTH, DROWN y SWEET32).

Existen páginas Web que pueden identificar la calidad con respecto a la seguridad de navegadores Web (https://www.ssllabs.com/ssltest/viewMyClient.html) y donde existen otros proyectos relacionados con la seguridad Web (https://www.ssllabs.com/projects/index.html).

De acuerdo con ello, se pide:

Apartado 3). Proceso para la comprobación y en su caso de las correspondientes modificaciones de las configuraciones de los navegadores. El Hospital dispone **de dos tipos diferentes de navegadores (Chrome y Firefox)** que aceptan conexiones SSL/TLS, debemos comprobar que están configurados para no aceptar conexiones con algoritmos de cifrado/integridad débil y/o versiones obsoletas del protocolo. Se debe destacar en este punto que una conexión SSL/TLS no es segura porque se escriba https:// antes de la dirección web. Nos consultan sobre el **PROCESO QUE DEBE SEGUIRSE PARA ASEGURAR LOS NAVEGADORES RESPECTO A LA SEGURIDAD EN GENERAL**. **(Valoración 20%)**

Apartado 4). Caracterización de los ataques BEAST (CVE-2011-3389), CRIME (CVE-2012-4929), PODDLE (CVE-2014-3566), FREAK (CVE-2015-0204), DROWN (CVE-2016-0800), SWEET32 (CVE-2016-2183). Sobre el protocolo SSL/TLS en que se apoya la seguridad del protocolo https existen múltiples tipos de ataques muy bien identificados, por ejemplo el ataque CRIME está relacionado con la fuga de información cuando los datos se comprimen antes de cifrarse y trabaja contra las cookies de sesión. Si un man-in-the-middle (MITM) puede observar el tráfico de red y manipular el navegador de la víctima para enviar solicitudes al sitio Web objetivo, podría

robar las cookies del sitio Web (se pueden descifrar las cookies), y por tanto secuestrar la sesión de la víctima. La consulta **consiste en presentar un informe con la información siguiente**. **(Valoración 20%)**

Tipo de Ataque	Causa del ataque	Efecto del ataque	Contramedidas recomendadas	Equipos
BEAST				Todos
CRIME				Impares
POODLE	Uso de cifrado CBC y servidor indica padding OK/incorrecto	Se obtiene el texto plano a partir del texto cifrado	No uso de SSL, sino TLS. Uso de GCM.	Todos
FREAK				Pares
DROWN				Impares
SWEET32				Pares
Nuevo CVE relacionado con la seguridad				Todos