La Esteganografía, el viajero ‘oculto’ de la Criptología. Historia aplicada a la informática. Casos prácticos.

Publicado en 20 julio, 2012, por oscardelacuesta en Criptografía, Historia, Ingeniería del Software, Seguridad, Software, Varios.

La **esteganografía** (del griego *στεγανος* (*steganos*) :cubierto u oculto, y *γραφος* (*graphos*): escritura), es la parte de la criptología en la que se estudian y aplican técnicas que permiten el **ocultamiento de mensajes u objetos, dentro de otros**, llamados **portadores**, de modo que no se perciba su existencia.

La **ventaja** de la rama de la ciencia, en comparación con la sola criptografía, está que los mensajes elaborados por la esteganografía **no atraen atención a sí mismos**. Los mensajes cifrados, aunque robustos, engendran sospechas y pueden ser incriminatorios en países donde la criptografía es ilegal. Por lo tanto, mientras que el cifrado protege el contenido de un mensaje, puede decirse que la esteganografía **protege mensajes y ambas las partes de la comunicación.**

Es decir, se trata de ocultar mensajes dentro de otros y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase **inadvertido** para observadores que tienen acceso a ese canal.

En este Post veremos sus utilidades y como implementar dichos algoritmos …

La esteganografía (en inglés Steganography) se conoce desde tiempos inmemoriales, teniendo los primeros referentes en la antigua Grecia, se ha empleado con éxito a lo largo de toda la Historia con distintos procedimientos y en particular durante la II Guerra Mundial.

Considerémoslo pues como el arte y ciencia de escribir mensajes secretos de tal forma que **nadie fuera de quien lo envía y quien lo recibe** sabe de su existencia; en **contraposición** con la criptografía, en donde **la existencia del mensaje es clara**, pero el contenido del mensaje está oculto. Por lo general un mensaje de este tipo parece ser otra cosa, como un texto, un artículo, un cuadro, una foto, archivo de música, vídeo etc. pero realmente oculta algo al resto.

Algunos ejemplos de técnicas de esteganografía que han sido usados en la historia son:

– Mensajes ocultos en tabletas de cera en la antigua Grecia, la gente escribía mensajes en una tabla de madera y después la cubrían con cera para que pareciera que no había sido usada.

– Mensajes secretos en papel, escritos con tintas invisibles entre líneas o en las partes en blanco de los mensajes.

– Durante la segunda guerra mundial, agentes de espionaje usaban micro-puntos para mandar información, los puntos eran extremadamente pequeños comparados con los de una letra de una máquina de escribir por lo que en un punto se podía incluir todo un mensaje.

– Mensajes escritos en un cinturón enrollado en un bastón, de forma que sólo el diámetro adecuado revela el mensaje. El escitalo es una vara de madera sobre la que se enrosca una tira de cuero o de pergamino, tal como se muestra en la Figura siguiente:

Cuando se desenrosca del escitalo (vara de madera) del emisor, la tira de cuero parece llevar una lista de letras al azar: S, T, S, F… Sólo al volver a enroscar la tira alrededor de otro escitalo con el diámetro correcto reaparecerá el mensaje.

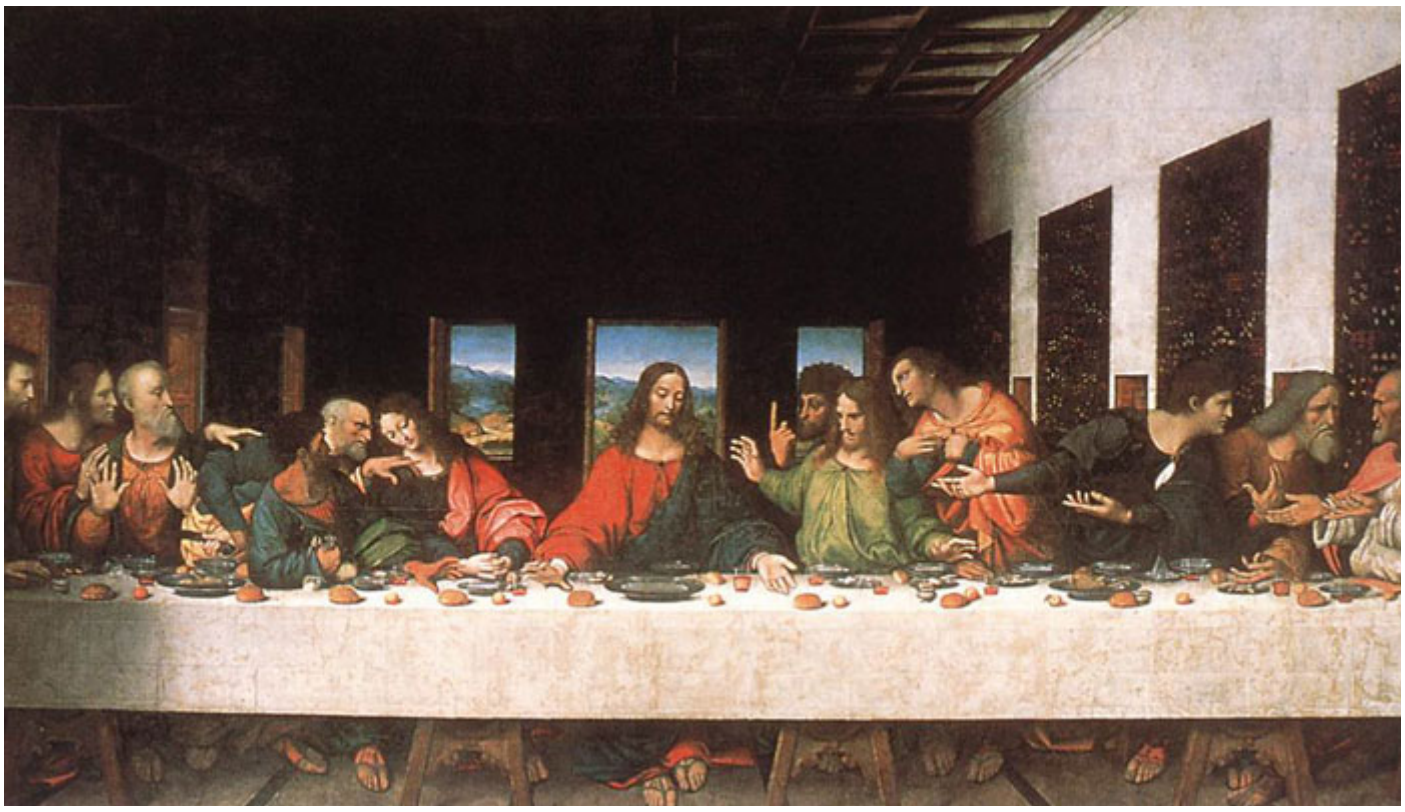
En el año 404 a.c. se presentó ante Lisandro de Esparta un mensajero, maltrecho y ensangrentado, uno de los cinco únicos supervivientes del arduo viaje desde Persia. El mensajero le dio su cinturón, y Lisandro lo enrolló en su escitalo, enterándose así de que Farnabazo de Persia planeaba atacarlo. Gracias al escitalo, Lisandro se preparó para afrontar ese ataque y lo repelió.

Busto de Lisandro

– Mensajes escritos en el cuero cabelludo, que tras crecer el pelo de nuevo, oculta el mensaje. Aunque este tipo de ocultación no es

aplicable en mi caso 😉

Unos de los grandes steganografos de la historia ha sido sin dudas el gran **Leonardo Da Vinci**. De ahi que se hizo tan popular, entre otras cosas, el código Da Vinci. De hecho la imagen destacada del POST intenta metaforizar dicho concepto.



¿ Realmente ocultó Leonardo algo en la última cena?,como veremos puede que **yo** sí.

Conocer la Historia nos ayuda a conocernos a nosotros mismos, aprender de lo vivido, y digo esto, porque una vez, realizada esta introducción, os mostraré algún caso práctico aplicado, con herramientas informáticas.

Como dato relevante es necesario considerar que **La esteganografía es razonablemente segura para intercambiar información en la red,** y más aún en redes sociales.

Lo primero que hay que indicar, es percatarnos que si realizamos una búsqueda por ejemplo en Softonic, de este tipo, enlace , se muestran 22 programas relacionados, casi todos ellos gratuitos .

La esteganografía asociada a las aplicaciones informáticas, tiene varias utilidades y se aplica generalmente a: música, imágenes, archivos comprimidos. Ejemplos zip, rar, mp3, textos.

A continuación estudiaremos todos estos conceptos con el programa libre OpenPuff:

Enlace de descarga de la web del autor: http://embeddedsw.net/OpenPuff_Steganography_Home.html

OpenPuff Steganography and Watermarking, a veces abreviado en **OpenPuff** o **Puff**, es una herramienta libre de esteganografía para Microsoft Windows creada por **Cosimo Oliboni** y todavía desarrollada como software independiente. El programa es notable por haber sido uno de los **primeros instrumentos de esteganografía** (versión 1.01 liberada el diciembre de 2004) que:

- permite que los usuarios escondan datos en más que un solo portador. Cuando los datos ocultos se distribuyen entre un juego de portadores forman una cadena, sin algún límite del tamaño teórico (256MB, 512MB, … depende sólo de la implementación)
- implementa 3 niveles de ofuscación de los datos ocultos (criptografía, whitening y encoding)
- extiende la criptografía negable en la esteganografía negable

La última revisión soporta una gama amplia de formatos de portadores, denominados carriers:

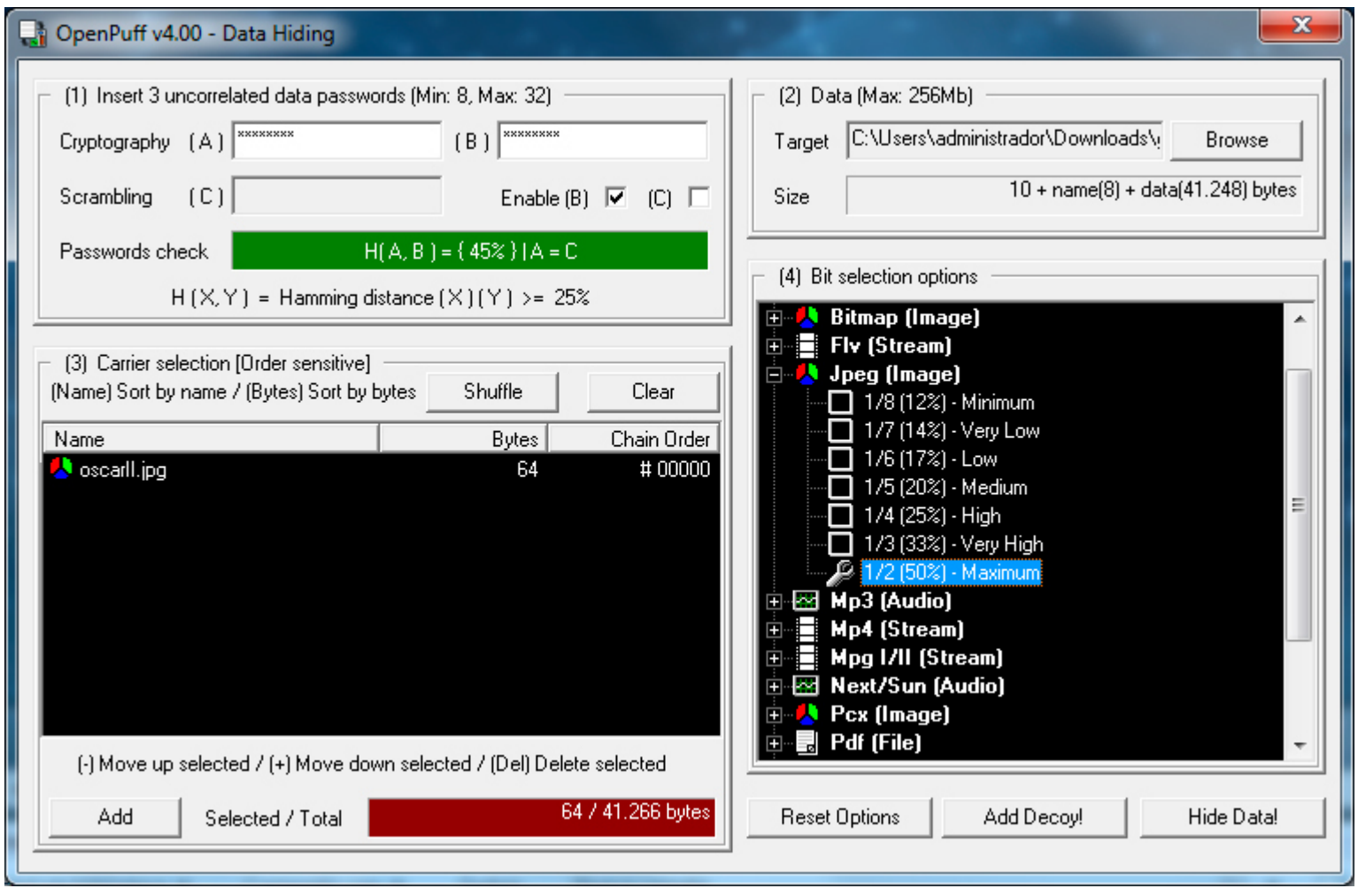
- Archivos de imagen Bmp, Jpg, Png, Tga
- Archivos de audio Aiff, Mp3, Wav
- Archivos de video 3gp, Mp4, Mpeg I, Mpeg II, Vob
- Archivos de Flash-Adobe Flv, Pdf, Swf

Una vez instalado, abre el programa.

Verás una pantalla como esta

Pulsa el botón – Hide – Ocultar.

Manos a la obra …



Existen 3 campos de contraseñas, sólo es obligatorio marcar una, el resto es necesario para dar más seguridad.

Desactivamos la casilla B, para este tutorial de ejemplo.

Usamos una password de al menos 8 caracteres.

En este momento, que considero **más difícil de interpretar por parte del programa**, ya que no se encuentra muy bien explicado, seleccionamos el archivo donde vamos a meter el fragmento oculto. Es decir **la madre**. Aunque sea el punto 3 es necesario realizarle antes que el 2.

Acto seguido, debemos seleccionar las opciones del tipo de archivo madre elegido en el punto 4. Si seleccionamos un JPG, tenemos que marcar las opciones relativas al JPG que permiten ajustar el ratio. Esto es importante tenerlo en cuenta en el proceso inverso esteganografico.

Por último en el punto 2: Data:, seleccionamos el archivo a proteger. Y pulsamos el botón Hide u ocultar. Esto nos permitirá elegir un directorio donde depositar el archivo generado (en su interior el archivo oculto).

Podemos comprobar cómo el nuevo archivo generado sigue siendo el mismo y permite hacer las mismas funciones. Si es un mp3, sigue sonando igual, si es una imagen se ve de la misma forma que la original, etc.

Para rescatar el archivo es necesario realizar el mismo proceso pero a la inversa, eso si, conociendo la contraseña y el tipo de archivo solapado.

Se usa OpenPuff principalmente para intercambiar datos de forma asincrónica y anónima:

El emisor trasmite un flujo de datos escondidos dentro de algunos portadores públicamente disponibles (contraseña + portadores+ orden de los portadores constituyen la clave secreta) el receptor recupera el flujo de datos ocultos usando la clave secreta.

Watermarking o marca de agua digital es la acción de firma un archivo con un ID que certifica el derecho de propiedad . OpenPuff lo hace en una manera esteganográfica invisible, aplicando la esteganografía a cualquier formato de portador soportado. La marca invisible no está protegida por contraseña y es accesible por todos (usando el programa).

Aplicación matemática.

La idea que sigue la esteganografía es enviar el mensaje oculto (E) “escondido” en un mensaje de apariencia inocua (C) que servirá de “camuflaje”. Esto es, se aplica una función de esteganografía $f(E)$.

El resultado de aplicar la función (O), se envía por un canal inseguro y puede ser visto sin problemas por el guardián. Finalmente, el otro prisionero recibe el objeto O y, aplicando la función inversa $f^{-1}(O)$, puede recupera el mensaje oculto.

La Inserción del Bit menos significativo, es el método moderno más común y popular usado para esteganografía, también es uno de los llamados **métodos de sustitución**.

Consiste en hacer uso del bit menos significativo de los pixels de una imagen y alterarlo. La misma técnica puede aplicarse a **vídeo y audio**, aunque no es lo más común. Hecho así, **la distorsión de la imagen en general se mantiene al mínimo** (la perceptibilidad es prácticamente nula), mientras que el mensaje es **esparcido a lo largo de sus píxeles**. Esta técnica funciona mejor cuando el archivo de **imagen es grande,** posee fuertes variaciones de color (“imagen ruidosa”) y también aventaja cuanto mayor sea la profundidad de color. Asimismo esta técnica puede utilizarse eficazmente en imágenes a escala de gris, pero no es apropiada para aquellas en color de 8 bit paletizadas (misma estructura que las de escalas de gris, pero con paleta en color). En general, los mejores resultados se obtienen en i**mágenes con formato de color RGB** (tres bytes, componentes de color, por pixel).

Lo que la esteganografía esencialmente hace es explotar las limitaciones de la percepción humana, ya que los sentidos humanos no están capacitados para buscar archivos que tienen información escondida dentro de ellos.

Resumiendo

Para terminar, es necesario aclarar que su uso, debe ser **responsable y legal**. En internet existe conocimiento de esta técnica que es empleada en muchas ocasiones y por muchas organizaciones para el intercambio de archivos ilegales y **delictivos**.

Es por ello que existen utilidades para comprobar que un archivo determinado, tiene solapado algo. Como una especie de análisis que emplean los cuerpos de seguridad para detectar actuaciones más allá de lo lícito. Esto se denomina (otro palabro) **Estegoanálisis y es la ciencia dedicada al estudio de la detección de mensajes ocultos.** Hablar sobre este otro concepto es otro mundo, puedes encontrar más información **aqui.**

Espero que este POST sea de vuestro interés. **Chao**.

Más información sobre OpenPuff: http://es.wikipedia.org/wiki/OpenPuff