

Esteganografía

Fecha: 26/03/2006

Fuente: www.lordepsylon.net

El objetivo principal del proyecto es mostrar la existencia de un método de camuflaje de información muy útil y sencillo.

<esteganografía: del griego "steganos" (secreto) y "grafía" (escrito). También llamada cifra encubierta >

Es 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 contraste con la criptografía, en donde la existencia del mensaje es clara pero está oscurecido. Por lo general un mensaje de este tipo parece ser otra cosa, como una lista de compras, un artículo, una foto, etcétera.

Los mensajes en la esteganografía muchas veces son cifrados primero por medios tradicionales, para posteriormente ser ocultados por ejemplo en un texto que pueda contener dicho mensaje cifrado, resultando el mensaje esteganográfico. Un texto puede ser manipulado en el tamaño de letra, espaciado, tipo y otras características para ocultar un mensaje, sólo el que lo recibe, quien sabe la técnica usada, puede extraer el mensaje y luego descifrarlo.

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

Mensajes ocultos en tabletas de cera en la antigua Grecia (en tiempos de Herodoto) , la gente escribía mensajes en una tabla de madera y después la cubrían con cera para que pareciera que no había sido usada. Existe una historia que describe como enviaron un mensaje a Esparta para avisar de que Xerxes tenía intención de invadir Grecia

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.

Mensajes escritos en el cuero cabelludo, que tras crecer el pelo de nuevo, oculta el mensaje.

Con la llegada de los ordenadores se han ampliado y diversificado las técnicas esteganográficas. Una de las más comunes consiste en ocultar un mensaje dentro de contenidos multimedia, mezclando los bits del mensaje original entre los bits del archivo gráfico o de sonido. El archivo resultante será una imagen o archivo de audio totalmente funcional que, a primera vista, no levanta ninguna sospecha, pero con el software adecuado es posible extraer la información oculta.

Se cree que esta técnica de ocultación de mensajes fue usada por los causantes del ataque a las

torres gemelas de Manhattan en Nueva York el 11 de Septiembre del 2001. Gracias a ella establecieron comunicaciones a través de Internet sobre sus futuros planes de manera sencilla y sin levantar ninguna sospecha.

Para utilizarla, se escoge un fichero, un documento Word, un documento PDF, una imagen BMP, un archivo de sonido .WAV o .MP3 que nos sirva como contenedor, y luego se crea el mensaje o el fichero que se desea ocultar. El programa que realiza la ocultación, modificará la portadora de varias formas posibles, alterando los valores de algunos de los puntos de la imagen, sumándoles o restándoles 1 (+1 para indicar el bit 1 y -1 para indicar el bit 0), de forma que sea imperceptible, pero que alguien que sepa que en esa imagen hay un mensaje, pueda recuperarlo. Otra forma de codificarlo es usar partes "no usadas" del fichero, por ejemplo, dentro de la cabecera del fichero hay a veces unos cuantos bytes que se dejan para uso de versiones posteriores, o después de la marca de fin de fichero, se puede añadir más información, sin que ningún de los programas habituales lo detecten. Existen métodos más robustos que usan tramas para el fondo de las imágenes, o alguna modulación determinada para el sonido, y conservan el mensaje aunque se cambie de tamaño o se pase a analógico.

Esta técnica se suele usar bastante para realizar "marcas de agua", es decir, para que cuando uno vea una imagen, sepa que procede de un sitio determinado.

Uno de los programas más populares y sencillos para realizar esteganografía básica es Stego o su front-end WinStego (concretamente envían mensajes sobre texto plano). Ambos se encuentran liberados bajo la licencia GPL por tanto se consideran Software Libre. Stego está disponible para Windows y para Linux, y puede compilarse para cualquier otra plataforma. El software es español, a pesar de encontrarse en inglés.

Para descargar el programa haz click en el siguiente link

<http://francyzone.onlywebs.com/download.php> y elige la última versión acorde con el Sistema Operativo que uses.

Para Enviar un mensaje secreto con WinStego haremos lo siguiente:

1º Crear un texto plano bien justificado

2º Pegar dicho texto en el cuadro de edición marcado como TXT. WinStego dispone de un botón Paste que quitará cualquier texto anterior de dicho cuadro y pegará el contenido del protapapeles.

3º Introducir el mensaje secreto en el cuadro de edición marcado como MSG. Este mensaje es el que se quiere que sea secreto, y que nadie conozca. Además el tamaño que admite depende de la longitud del texto introducido como TXT.

4º Elegir el método, por ahora solo hay una posibilidad -tj (texto simple justificado).

5º Eligir el número de columnas que tendrá el texto y se introduce en el recuadro marcado con BPL (bytes por línea). Por defecto el programa lo fija en 70, lo cual es adecuado para enviar el mensaje por correo electrónico.

6º Para usar cifrado se marca la opción password, lo que hace que nos pida la clave de cifrado antes de codificar o decodificar el mensaje. El cifrado usado por stego es IDEA en modo CFB-8 lo que permite cifrar mensajes de cualquier longitud múltiplo de un byte sin añadir bytes extras (internamete no usa la password proporcionada sino el el resumen MD5 de la misma que se

corresponde con los 128 bits de clave del algoritmo IDEA).

7º Pulsar el botón Encode, y ya tenemos el resultado en el recuadro TXT.

8º Copiar el texto resultante, para lo cual podemos usar el botón Copy.

9º Enviar el texto resultante por correo electrónico o cualquier otro método que consideremos oportuno.

Para Recibir un mensaje secreto con WinStego haremos lo siguiente:

1º Pegar el texto codificado en el cuadro de edición marcado como TXT.

2º Elegir el método, por ahora no se puede ya que solo hay uno.

3º No es necesario modificar BPL ya no es necesario conocerlo para poder decodificar el mensaje.

4º Para usar cifrado se marca la opción password, lo cual hará que nos pida la clave usada en el momento de codificar el mensaje.

5º Pulsar el botón Decode, y ya tenemos el mensaje secreto en el recuadro MSG.

Es fascinante observar hacia donde puede avanzar la esteganografía, imaginemos que podemos usar el código genético de una bacteria, por ejemplo, para ocultar mensajes, con la facilidad que tienen las bacterias para reproducirse, tendríamos miles de copias de un mensaje en segundos. Si esa bacteria es la de la gripe. Fácilmente sabrías que has recibido un mensaje cuando comiences a tener los síntomas de dicha enfermedad. Sabiendo que has recibido un mensaje solo te queda descifrarlo, recoges una muestra del ADN de la bacteria de tus fosas nasales, lo analizas y obtienes el mensaje oculto.

"No dejes que te analicen, sin al menos poner algún obstáculo "

<Lord Epsilon>