ESTEGANOGRAFIA

Gonzales Marin Libia Karina
Universidad Mayor de San Andrés
Carrera de informática
Análisis y Diseño de Sistemas de Información
Libita_07@hotmail.com

RESUMEN

El siguiente artículo hace mención a la esteganografía, la cual es una técnica utilizada por el ethical hacking y sirve para crear mensajes cifrados de manera tal que no se muestre ni se pueda detectar y está asociado a un cifrado de mensajes.
Esta técnica es generalmente utilizada para ocultar información o cifrarla de tal manera que no pueda ser vista o descubierta por algún "intruso" o sujeto para el cual esa información no esté dirigida, logrando así que el intercambio de información sea discreta y segura para quienes la realizan.

TERMINOS GENERALES

Esteganografía, ejemplo de esteganografía, clasificación según su tipo de estego-algoritmo, esteganografía pura, esteganografía de clave secreta, esteganografía clásica vs. Esteganografía moderna

Palabras clave

Ehtical Hacking, Esteganografía, información cifrada, información.

1. INTRODUCCION

La esteganografía es una técnica que permite entregar mensajes camuflados dentro de un objeto (contenedor), de forma que no se detecte su presencia y pasen inadvertidos. Asociada con cifrado de mensajes, la esteganografía puede ser útil para almacenar datos en la nube que queramos tener disponibles desde cualquier lugar.

En el campo de la esteganografía digital es posible ocultar información en todo tipo de soportes como archivos de audio, imágenes, vídeos, textos, etc.
Una forma muy conocida es la del bit menos significativo (LSB) que pertenece a los llamados métodos de sustitución, consistente en ocultar el mensaje en el bit menos significativo de un archivo, generalmente una imagen aunque es aplicable a más soportes, de forma que el cambio en el fichero original sea casi imperceptible.[1]

2. Cómo funciona la Esteganografía

Como ejemplo clásico para ilustrar la utilidad de esta disciplina, supongamos que dos presos en una prisión están planeando su huida pero el único método que tienen para comunicarse es por medio de mensajes escritos que han de pasar por un guardia de seguridad como intermediario que evaluará su contenido antes de hacer llegar el mensaje a su destinatario. Si uno de ellos quiere enviarle un mensaje al otro preso contándole que la huida será mañana no podrá escribir el mensaje tal cual puesto que el guardia intermediario evitará que llegue a su destino y además tomará medidas. Tampoco deben enviar el mensaje encriptado porque el guardia lo encontrará sospechoso (símbolos sin ningún sentido aparente como mensaje). La opción más adecuada es pues, ocultar el mensaje con la información de la huida dentro de otro mensaje (al que se le denomina portador), entonces el preso emisor decide esconder el mensaje en cada letra del final de las frases, quedará entonces un mensaje de apariencia común, sin relevancia, sin embargo el preso receptor al unir las letras del final de las frases encontrará la información sobre la huida sin que el intermediario haya sospechado nada. [1]

Pero si el guardia ya se hubiese imaginado algo así y decidiese alterar el contenido del mensaje para destruir cualquier posible información oculta este método no sería válido. Surgen pues los mensajes esteganográficos que soportan las alteraciones en el medio en el que están expuestos, es decir aunque se modifique el contenido del mensaje aparente sigue estando la información original oculta. A esto se le conoce como esteganografía robusta, muchos autores la denominan como "marcas de agua" y la diferencian de la esteganografía común (la que es vulnerable a las distorsiones en el medio).

3. Clasificación según el estego-algoritmo.

El estego-algoritmo es el algoritmo esteganográfico que indica cómo realizar el procedimiento de incorporación del mensaje esteganográfico en el portador para obtener el estego-mensaje. Según el tipo de estego-algoritmo podemos distinguir entre dos tipos de esteganografía[4]: Esteganografía pura y esteganografía de clave secreta.

3.1 Esteganografía pura

En este tipo de esteganografía el estego-algoritmo establece un método fijo para incorporar el mensaje esteganográfico en el portador para obtener el estego-mensaje. En esta estrategia se está suponiendo que el guardián del problema del prisionero no conoce nada sobre el estego-algoritmo. Por tanto estamos basando nuestra seguridad en la oscuridad. Este enfoque para conseguir la seguridad raramente funciona y es especialmente desastroso en el caso de la criptografía.

3.2 Esteganografía de clave secreta

En este tipo de esteganografía el estego-algoritmo está parametrizado por una clave esteganográfica a la que se le llama estego-clave que define como aplicar el algoritmo: Por ejemplo, la estego-clave podría indicar el lugar dentro del portador a partir del cual se comienza a realizar la incorporación del mensaje secreto. Tanto el estego-algoritmo como la estego-clave deben estar previamente acordadas entre el emisor y el receptor.

El proceso de extracción consiste en aplicar el estego-algoritmo y la estego-clave necesarios al estego-mensaje recibido para obtener el mensaje esteganográfico.

En este escenario el guardián del problema del prisionero puede conocer el estego-algoritmo pero no conoce la estego-clave, que se emplea en el mismo. En esta estrategia estamos basando nuestra seguridad en el principio de Kerckhoffs. Aplicado a la esteganografía, el principio de Kerckhoffs podría incluir como información revelable, el acceso a la información portadora antes de aplicársele el estego-algoritmo.

4. Esteganografía Clásica vs. Esteganografía Moderna

Esteganografía "clásica": está caracterizada por sus métodos completamente oscuros**,** o sea de manera manual y sin una fuente tecnológica.

- Protección basada en desconocer el canal encubierto específico que se está usando.

Esteganografía moderna: caracterizada por el uso de tecnología digital o canales digitales:

- Archivo de texto (inc. páginas web, código fuente, etc.)
- Audio digital
- Imágenes yvídeo digitales
- Archivosejecutables
- Protocolos de comunicaciones

5. PROGRAMAS PARA REALIZAR LA ESTEGANOGRAFIA

5.1. Camouflage: el programa que popularizó la esteganografía

En la actualidad existen varios programas que sirven para poner en práctica la esteganografía, pero hace más de diez años uno destacaba sobre los demás: Camouflage (véase figura 1).

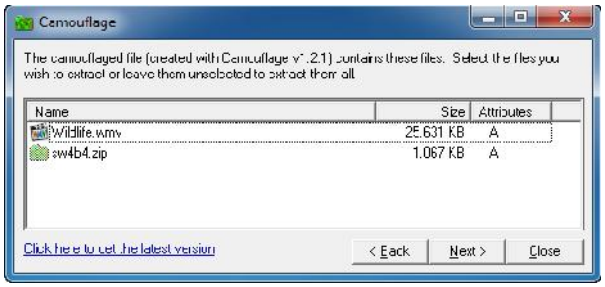

Figura 1. Ventana del programa camouflage

Su razón de ser es muy actual: **proteger mensajes y archivos personales** de miradas curiosas, en concreto, de los dueños de servidores web o de servidores de correo que guardaban estos archivos.
Aunque hoy en día se comparte prácticamente todos los datos y archivos, a través de redes sociales y de servicios como Dropbox o Mediafire, en ocasiones es necesario proteger ciertos documentos.
El funcionamiento de Camouflage es bastante sencillo, tanto que no tiene ventana principal en sí sino que **se activa** desde el menú contextual**,** seleccionando los archivos a ocultar.
Desde un asistente, Camouflage te guía paso a paso para elegir el archivo que verán todos en vez del fichero ocultado y te da la opción para añadir una contraseña.
Y para descubrir el archivo oculto, basta con seguir el mismo proceso con el menú contextual.

5.2. Otros programas de esteganografía

Camouflage dejó de actualizarse hace tiempo, aunque funciona tan bien como el primer día. Pero si buscas programas más actuales, te damos una lista. La mayoría están especializados en ocultar archivos detrás de imágenes, pero algunos son más genéricos y admiten todo tipo de ficheros.

- FileInyector
- Bon Kyu Bon
- Plain Sight
- Hide & Reveal
- PicCrypt
- P2Stego.[5]

6. CONCLUSIÓN

La esteganografía es muy eficiente y muy buena opción a la hora de ocultar información si es necesario, como se pudo observar en el artículo, existen programas para realizarlo y se puede observar que no existe solo una manera de emplearla ya que está basada en un estego-algoritmo además de haberse modificado y modernizado a través de los años gracias al avance tecnológico de la ciencia. También es necesario subrayar que es una técnica muy buena y de gran ayuda a la hora del intercambio de información secreta, pero también es un modo peligroso de manejo de la

información ya que esta técnica puede ser usada con otros fines o de manera inadecuada.

7. REFERENCIAS

Título: Anónimo
Autor: Introducción a la esteganografía:
Disponible en: http://manualesgeek.blogspot.com/2011/06/introduccion-la-esteganografia.html
Fecha de acceso: 23/05/13 Hrs. 19:10

Cuaderno de notas del observatorio, Esteganografía el arte de ocultar información.
Autor: Anónimo.
Disponible en: http://www.taringa.net