Universidad de Granada

DEPARTAMENTO DE ÁLGEBRA

Criptografía

Esteganografía

Esteganografía

Autores: Alexander Moreno Borrego
Carlos Jesus Fernandez Basso

Correos: alexmobo@correo.ugr.es
karloos@correo.ugr.es

DNI: 39906263-K
75927137-C

Profesor: Jesús García Miranda

Contenido

Introducción

¿Qué es la esteganografía?

El termino esteganografía viene del griego *στεγανος* (steganos): cubierto u oculto, y *γραφος* (graphos): escritura.

A diferencia de la criptografía, que transforma el mensaje original para que nadie más que el receptor puede hacer la transformación inversa y entenderlo, la esteganografía oculta el mensaje original para que no pueda verse a simple vista pero no lo transforma de ninguna manera.

Estos mensajes se escribían, en claro a través de un canal encubierto no encriptado, dentro de otros, llamados portadores, de manera que no se percibiera si existencia. Se pretendía, incluso, que el propio hecho de la comunicación pasara inadvertido.

Terminología básica

El conjunto de componentes necesarios que permiten llevar a cabo la comunicación esteganográfica se denomina **esquema esteganográfico**.

- El **portador** es todo aquel conjunto de datos que es susceptible de ser alterado para incorporarle el mensaje que queremos mantener en secreto.
- Un **mensaje-legítimo** es el mensaje transportado por el portador.
- Se llama **mensaje esteganográfico** al mensaje que queremos mantener en secreto y queremos esconder dentro del portador.
- **Estego-algoritmo** es el algoritmo esteganográfico que indica cómo realizar el procedimiento de incorporación del mensaje que queremos mantener en secreto en el portador.
- La acción de ocultar el mensaje dentro del portador se denomina **embeber**.
- **Estego-mensaje** al resultado de embeber el mensaje esteganográfico dentro del portador.
- La acción de la recuperación, a partir del estego-mensaje, del mensaje oculto esteganográfico se denomina **extraer**.
- El emisor es también llamado **embebedor** y el receptor **extractor**.

- Se llama **esteganalista** o **estegoanalista** a la persona que intenta determinar la existencia o ausencia de un mensaje esteganográfico. Basta con determinar la existencia. Es el que hace **estegoanálisis**.
- Los **canales de selección** consisten en canales adicionales al portador utilizado para embeber donde se comunica qué posiciones del portador se utilizan para la comunicación esteganográfica.
- Las **clases de equivalencia** corresponden a pares de elementos del portador utilizado que tienen una interpretación semántica equivalente en la comunicación legítima, pero el uso de un elemento u otro tiene un significado acordado en la comunicación esteganográfica.

Esteganografía clásica (historia)

Para poder ilustrar bien la esteganografía clásica lo mejor es poner algunos ejemplos de la evolución de la misma durante la historia.

Allá por el 600 a.C., en China se escribían mensajes en una tela muy fina, se hacía una bola y se recubría con cera. Después se engullían las bolas de cera.

Unos 200 años más tarde, sobre el 400 a.C., tenemos uno de los ejemplos más antiguos de los que se tiene constancia lo explica Heródoto, en *Las historias*. En él, cuenta dos historias o métodos que pueden clasificarse como esteganografía:

1. Un personaje coge dos tablillas de madera cubiertas de cera y les quita la cera. Seguidamente, graba un mensaje en la madera y las cubre con cera tal y como estaban anteriormente.
2. Otro personaje le rapa la cabeza a su esclavo y le tatúa el mensaje en la cabeza. Cuando le crece el pelo manda el esclavo al receptor con el mensaje de que le rasuren la cabeza.

Siglos más tarde, en el siglo XV, un científico italiano descubrió cómo esconder un mensaje en un huevo duro, el científico se llamaba Giovanni Battista della Porta. Se mezcla una onza de alumbre y una pinta de vinagre y se escribe en la cáscara con ello. El mensaje sólo se puede leer pelando el huevo duro.

A principios del siglo XVI se acuña la palabra esteganografía. Un abad alemán, Johannes Trithemius, escribió un libro sobre el tema que estamos tratando, la ocultación de información, y lo llamó *Stheganographia*.

Un ejemplo de mensaje escondido dentro de otro es el siguiente:

- Francesco Colonna escribió el libro *Hypnerotomachia Poliphili*, si se cogen las primeras letras de todos los capítulos del libro se puede leer el mensaje "El hermano Francesco Colonna amó apasionadamente a Polia".

Ya más tarde, durante la segunda guerra mundial se buscaron muchas maneras de ocultar la información por parte de todos los bandos. Se usaron microfilmes en los puntos de la íes y en los signos de puntuación para enviar mensajes secretos.

Null cipher

También se utilizó una técnica llamada *Null Cipher* (Cifrado nulo) que consistía en esconder un mensaje en otro lo más común y corriente posible. El ejemplo siguiente lo muestra perfectamente:

Apparently neutral's protest is thoroughly discounted
and ignored. Isman hard hit. Blockade issue affects
pretext for embargo on by products, ejecting
suets and vegetable oils.

Si extraemos la segunda letra de cada palabra tenemos el siguiente mensaje:

Pershing sails from NYr June I

Tinta invisible

La tinta invisible es una técnica que no está claro desde cuando se utiliza, lo que sí está claro es que se ha utilizado a lo largo de la historia y aún se utiliza. Se utilizaba mucho por la resistencia en los campos nazis. Se pueden clasificar en dos categorías diferentes:

- Básicas: Las sustancias con alto contenido en carbón reaccionan al calor y se oscurecen las superficies donde se han utilizado esas sustancias (sustancias como la leche, la orina, el zumo de limón, de naranja, de manzana, de cebolla, alguna solución azucarada, la miel diluida, la coca cola diluida, el vino, el vinagre, etc).
- Químicas: aparecen tras una reacción química, o tras ser expuestas a la luz de cierta longitud de onda (IR, UV...).

Esteganografía moderna

La esteganografía moderna se basa en técnicas digitales, trata de ocultar la información en medios digitales.

Técnicas más usadas

Sustitución – Alteración/Reemplazo del LSB

Cuando se crea un archivo en un ordenador hay algunos bytes que no son realmente necesarios o, al menos, no muy importantes. Ahí es donde esta técnica esconde la información a ocultar.

Esta técnica funciona bien para archivos de imagen con una resolución muy alta o archivos de audio con un ratio de bit elevado. Normalmente no incrementa el tamaño del archivo, dependiendo del tamaño de lo que se quiera esconder.

Inyección

Esta técnica es más simple que la anterior ya que simplemente inserta directamente la información dentro del archivo.

Por ejemplo, después de la marca de EOF en un archivo, en los bloques de comentario de un fichero HTML o, un ejemplo más sencillo aún, una partición oculta en un disco duro.

Técnicas en los diferentes archivos

Archivos de texto

Un método muy fácil y efectivo es añadir espacios en blanco y tabuladores al final de las líneas, ya que en el modo normal de edición de la mayoría de los editores de texto no los muestra.

También es muy difícil detectar esta técnica esteganográfica por que los espacios en blanco son normales y naturales en los documentos de texto.

Imágenes

Para esconder información en las imágenes se usa la técnica LSB (*Less Significant Byte*). Para el ojo humano las pequeñas variaciones de un pixel son muy difíciles de detectar.

Audio

La técnica utilizada para esconder información dentro de los archivos de audio se llama *Low bit encoding.* El problema con ésta técnica es que muchas veces es sensible al oído humano y, por lo tanto, un método arriesgado.

Spread Spectrum es otro método que consiste en añadir ruidos aleatorios a la señal. La información se esconde en la portadora y se extiende por el espectro de frecuencias.

Por último, el método *Echo data hiding* usa los ecos del audio para esconder la información.

Video

Para esconder información dentro de un archivo de video se suele usar el método DCT (*Discrete Cosine Transform*). Este método funciona cambiando cada una de las imágenes que tiene el vídeo, DCT altera valores de ciertas partes de las imágenes, normalmente redondea al alza los valores.

Bibliografía

http://neobits.org/recursosexternos/death.pdf

http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

http://es.wikipedia.org/wiki/Esteganograf%C3%ADa

http://www.math.ucsd.edu/~crypto/Projects/MaxWeiss/steganography.pdf