Global Information Assurance Certification Paper

Steganography Policies for Protecting Your Web Site
Toni Borders
December 16, 2002
GIAC Security Essentials Certification (GSEC)
Option 1
Version 2

Abstract

In today's society where information is rapidly available through the Internet, your company has the ability to communicate through its web site to a worldwide audience. Although in reaching your vast audience, who has access to the World Wide Web, you can also leave your company incredibly vulnerable. Given the proper precautions, your company's web site will have a reduction in threats of malevolence. One major components of reducing risk is to implement a stenography policy into your company's existing security policy. In this paper I will explain an overall definition of steganography, steganalysis, what is to be included in the company's steganography policy, and steganography tools available for download. By understanding the high level explanations surrounding steganography, and implementing a policy, you will be able to increase protection to your company's web site.

Steganography Policies for Protecting Your Web Site

Your web site is a reflection of your hard work, and the image of your organization that visitors will see. Detecting any malicious intrusion on your web site has become increasingly difficult due to the rise of [1]**steganography**, the art of hiding messages in media in order to prevent recognition. Steganography is sometimes compared to cryptography, which creates a confidential message while still visible. [2]Steganography is different because it hides the very existence of the message. Basically, Cryptography jumbles a message in a way that if anyone captures the message the message cannot be comprehended. In contrast, an individual may not be aware that a steganography message had been sent, because it is hidden. Steganography may conceal an image inside an audio file, a video file, or another image file or it can hide audio or video data inside another audio or video file, or even inside a large image file. In other words, Steganography requires a host to carry its hidden message. Steganography is not limited to video, audio, images or text; it may also hide in spam, IP Headers or etc. The hidden messages may be text that can be represented as a bit stream. [3]The science of detecting, decoding, erasing, or altering messages hidden by steganography is called **steganalysis**.

Steganalysis is performed with the knowledge that steganography may reach their web site, and the understanding of steganography. [4]There are several techniques available for steganography. Steganography techniques extend from Least Significant Bit (LSB) to noise insertions, to the handling of images and

compression algorithms, to changes in image properties. Steganography exists when data is embedded, injected, or to use hidden data to create a new file. Steganography is growing rapidly, especially when it comes to image files. There are a number of easy to use Steganography tools available on the Internet to hide information in image files. Steganography tools are generally very easy to use, user friendly, and some that are free. Understanding the tools available for steganography, and just knowing that it exists assists steganalysis. Steganalysis is performed by a **steganalyst**.

Multiple factors combine to make steganalysis a difficult science. [4]First, the basic premise of steganography is that human observers will observe only the encapsulating media, and not the hidden message. This means that steganalyst must rely on technological detection of such messages, or knowing steganography techniques. The combination of new steganographic technology and abundant computing power has made it progressively easier to hide data in email, images, video and sound.

Steganography techniques used in hidden text are adding extra spaces, and breaks that your browser ignores. However if a steganalyst opens the source code the hidden text is revealed. Images can use a wide range of steganography methods to include: Least Significant Bit (LSB), noise insertions, manipulation of images and their properties, and compression algorithms. The easiest way to hide data is to replace the least significant bit of every element with on bit of the secret message. Images may also be embedded with Discrete Cosine Transformation (DCT), which can be applied to the entire image or just blocks of it. LSB and transformations can also be utilized for steganography purposes to audio and video. A steganalyst can detect steganography has been applied to audio and video by observing slight echoes, subtle signals or sounds of higher amplitude.

Steganography techniques also include hiding information by creating hidden partitions, and exploiting vulnerabilities in protocols. The steganalysis may detect hidden partitions through unusual or repetitive patterns without tools, using disk analysis programs to uncover unused areas and report on hidden information. Steganography also provides the tools for intruders to remove valuable or confidential information from your systems or to insert unauthorized data into them.

Reports of research of steganography scanners are being developed. However, no one can say with certainty whether stenography scanners have already have been developed, and are searching the net for hidden data. It is no exaggeration to say that steganography is a serious threat to the integrity of your web site and organization, and that steganalysis is vital to the reliability of the information contained on your web site. [5]Wetstone has developed a product called Stego Watch, designed to allow users to detect digital steganography, or the presence of communications hidden in digital files on your web site. Stego Watch initially

creates a baseline of your web site, and then continually scans it. Wetstone will handle the administration of Stego Watch or the user can administer the program. However, Stego Watch does not say if it can scan for all steganography and tools available.

[6]Steganalysis deals with detecting, extracting, and destroying steganography on your system, and in this paper's focus, your web site. Your job to detect steganography is difficult, but with the aid of the steganography knowledge, tools and a corporate steganography policy your job will be easier. Without steganography policies and procedures to protect your web site, the probability that steganography will invade it will increase as the Internet grows. Furthermore, strong network security alone cannot guarantee the safety of your systems; deficient internal security also provides the opportunity for steganography to infect them. [7]The best way for you to defend your systems is to implement steganography policies and procedures, and to assign the responsibility for enforcing them to one or more individuals. The steganography policy should be an essential part of your company's security policy.

Steganography policies should include:

- A policy on the use of stenographic programs, to alleviate the risk of employees using stenography on your company web site.

- A policy requiring images and text on the company's web site to have trusted digital watermarks, if any.

- Standards with the appropriate levels of heftiness, redundancy, and distribution to allow continued existence and recovery of encoded information even after distortion attacks.

- Implementation of secure directories of safe steganography images, video, audio and text files, which will be copied to the appropriate web pages by authorized individuals.

- Methods of compacting or compressing data rather than concealing it, which should be applied to the company's steganography.

- A set of approved tools for detecting the presence of steganography, as well as its effects (such as the distortion of embedded information).

- The disabling of self-executables, and the development of methods of distorting embedded data.

- Systems from registered application users to track stenographic media on your web site, and to maintain records of its characteristics in a database

so that transformation of original files can be located and control maintained.

- Steganographic systems and files to avoid detection by non-authorized personnel, as well as tools for circumventing these systems and files for computer forensics personnel.

- A policy requiring the cooperation of steganography staff, policies and procedures with network, web security, software and email policies.

- Any detection of unauthorized steganography must be reported to the security office immediately.

- A snapshot of the system, web site should be taken on the detection of steganography.

- Each incident of steganography will be dealt with individually, and documented in an incident log.

- Steganography, if used for illegal purposes will be subject to legal ramifications.

The implementation of the policies described above will enhance your ability to protect your web site, and will assist steganalysis by supplying approved tools.

[8]Many steganography tools are available for users with minimal knowledge of digital image format and coding techniques. These tools help the steganalyst better understand and appreciate some of the processes used by these tools. Steganography tools assist in understanding digital images, coding schemes and use of colors in digital images. This information also helps the steganalyst detect the presence of hidden information.

[9]Computer-based images are made up of an array of dots, called pixels that consists a very fine grid. Each pixel has its own color, represented internally as separate quantities of red, green and blue. Within Windows, each of these color levels may range between 0 and 255. Images may have eight bits per pixel or twenty-four bits per pixel. There are 256 color variations when you use eight bits per pixel, and 16,777 color variations when using twenty-four bits per pixel.

There are many steganography tools available for download via the Internet. I had listed some of the tools by their operating systems, and some source code that is available. Understanding that steganography tools are available and it what context they are available will help you understand what you at up against as a steganalyst.

Windows

Hide and Seek for Win95 (96k)
Hide and Seek is a BMP-based steganography program written by Colin Moroney. Mr. Moroney has written the Hide and Seek program in both Windows 95 and DOS versions. The interface makes Hide and Seek easy to use, and the file wiping options and blowfish header encryption method are of additional benefit. Regrettably, downloads are ITAR restricted, however, a 40-bit key version is available for international downloads.

Steganos for Win95 (1085k)
Deus Ex Machina Communications has written Steganos for Windows 95, which is an easy to use, powerful wizard style program to encrypt files and hide them within BMP, DIB, VOC, WAV, ASCII, and HTML files. Additionally, Steganos for Win95 implements a Shredder, which is a program that permanently wipes files from your hard disk.

[10]S-Tools4 (272k)
S-Tools v4 is a steganography tool that hides files in BMP, GIF, and WAV files. *Please note that this program will in the Windows 95 and NT environments.*

S-Tools3 (283k)
S-Tools3 is unique due to the fact that it hides files not only in BMP, GIF, WAV, but also in unused space on floppies! S-Tools3 performs well in the Windows operating systems.

Contraband (281k)
The Contraband program is exceptional, because this program embeds and extracts any conceivable file into 24-bit BMP's. The source code is available for Contraband.

PGPn123 (428k)
PGPn123 is predominantly a pgp "windows clipboard" shell program that exercises pgp for Eudora, Agent, or Pegasus Mail trouble-free. The latest version includes a steganography option that is put into operation after the message is pgp encrypted. The algorithm used in PGPn123 is based on the Texto program.

Scytale (575k)
Another pgp shell program is Scytale, which contains the added feature of hiding data in PCX images. Scytale also includes a built-in wiper and batch mode capabilities, which is an added benefit.

DOS

JSteg (462k)

JStegis is currently the only DOS program available for hiding data within the prevalent JPG format. Jsteg is an impressive program authored by Derek Upham. Before you can conceal data in a JPG file, you will need to save that file in the TGA (targa) format. Then once the data has steganography applied to the image, the consequential output file will be in the JPG format, with all of the compression advantages that JPG demands. Preston Wilson and Randall Williams have been kind enough to compile this DOS version, which has previously only been available for Unix. JStegis requires a support file placed in your path, which is available with the program.

Texto (59k)

Texto is a text steganography program, which is the only DOS implementation of the Unix source code by Preston Wilson. Texto converts uuencoded or PGP ascii-armoured data into English sentences. Texto requires this support file placed in your path.

GZSteg (346k)

PrestonWilson compiled GZSteg for DOS. This program is exceptional because it hides data in GZip compressed files. The GZSteg program requires a support file placed in your path.

Hide4PGP v1.1 (70k)

Hide4PGP v1.1 is a steganographic program that hides data within BMP, WAV, and VOC files. Hide4PGP v1.1 is designed to be used with both PGP and Stealth, however additionally works superior as a stand-alone program. Hide4PGP written by Heinz Repp is available in both a DOS and OS/2 executable. Hide4PGP v1.1's source code is included and should compile on any platform without major tribulations.

Steganos v1.4 (12k)

Steganos is a small, straightforward to use DOS source stego program that hides data inside BMP, VOC, WAV and ASCII files. The author of Steganos is Fabian Hansmann.

Pretty Good Envelope (25k)

Pretty Good Envelope (PGE) is a DOS based program that masks a message in another file by the very uncomplicated method of appending the message to the file. Then PGE appends a 4 byte little endian number, which points to the beginning of the message. The companion program UNPGE retrieves the message. PGE can be applied to graphic files (GIF and JPG) or any other binary files, including .COM and .EXE files.

Stealth (19k)
Stealth is a simple filter for PGP, which removes off all identifying header information to leave only the encrypted data in a format suitable for steganographic operations. The data can be hidden in images, audio files, text files, CAD files, and/or any other file type that may hold random data, and then transmitted to another person, who can retrieve the data from the file, attach headers, and PGP to decrypt the data.

Hide and Seek v4.1b (264k)
Hide and Seek v4.1b is a DOS based program for hiding data and seeking data using GIF image files. Hide and Seek v4.1b take data, usually text, including encrypted text, and hide it in a GIF file.

Hide and Seek v5.0 (199k)
This latest version of Hide and Seek has been totally redesigned. Although Hide and Seek is still a DOS based program, it now includes a user interface, which eliminates the command line operations to hide info in GIF files.

Snow (27k)
Snow is a text-based stego program that hides messages in text files by appending tabs and spaces on the end of lines. In Matthew Kwan's Snow, tabs and spaces are invisible to most text viewers, therefore the steganographic nature of this encoding scheme. Snow includes a compression function to allow you to stego more information into a given file and has some basic crypto functions via the ICE algorithm.

FFEncode (12k)
FFEncode is DOS program that "hides" a file in a text file by utilizing a "morse code" of NULL chararcters. To use FFEncode you should unpack the zip file and type FFENCODE or FFDECODE at the DOS prompt for the simple command line parameters.

StegoDos (22k)
StegoDos is a DOS based picture encoder that consists of a group of programs designed to allow you to capture a picture. Then encode a message in the picture, and show the picture so that it may be captured again into another format with a third-party program. Lastly recapture the picture and decode the message previously inserted inside it.

Wnstorm (84k)
Wnstorm (White Noise Storm) is a cryptography and steganography software package, which you can employ to encrypt and hide information within PCX images.

Java
EZStego Java
EZStego Java has similar steganographic functions as its Mac-based predecessor, but is written in the platform independent Java language. EZStego Java is currently it is being tested in an online version, this will allow you apply steganography from your web browser The author, Romana Machado plans to release the java code once the online testing is complete.

Macintosh
Stego (266k)
Stego is a steganography tool that enables you to embed data in Macintosh PICT format files, without changing the appearance or size of the PICT file. Stego can be applied as an "envelope" to hide a previously encrypted data file in a PICT file, creating detection a great deal less likely.

FatMacPGP 2.6.3
FatMacPGP 2.6.3 is the current version of MacPGP optimized for PowerMacs. FatMacPGP 2.6.3 has a Stealth option that removes all identifying header information to leave only the encrypted data in a format suitable for steganographic use.

Paranoid (80k)
Paranoid is primarily an encryption program that allows you to encrypt files with IDEA, triple DES, and an algorithm. Paranoid is a steganography program written by Nathan Mariels that allows you to hide files in sounds.

Amiga
Textego (41k)
Textego is Kevin Maher bases a substitution cipher on the Texto program.

OS/2
Hide4PGP v1.1 (70k)
Hide4PGP v1.1 is a steganographic program that conceals data within BMP, WAV, and VOC files. Hide4PGP by Heinz Repp is designed to be used with both PGP and Stealth, and additionally can be used as a stand-alone program.

Source Code
(Unix)
Snow - source code
Hide4PGP - source code
TCP/IP - source code
J4-jpeg - source code
Hide and Seek - source contained in zip file
Stealth (v1.2) - source code
White Noise Storm - source contained in zip file
Texto - source code for a text-based stego program
MandelSteg - source code for a gif-based stego program
Steganosaurus - source code for another text-based stego program

---

For this paper, I will focus on the Steganography tool S-Tools that utilize images. Understanding S-Tools will enable you do perform steganography and understand the functions. Additionally, S-Tools is incredibly easy to use even for a novice like myself, who does not like to read the instructions.

S-Tools hides information in images like Bitmap (BMP) and Graphic Interchange Format (GIF). S-Tools employs the LSB insertion method to hide the information within an image. LSB is the lowest bit in a series of numbers in binary, and is located at the far right of a string. The LSB method applies the binary representation of the hidden information and overwrites the LSB of each byte within the cover image. This is the change from the original image to the cover image.

Changes that introduce LSB insertion are almost imperceptible to human eye. S-Tools have known signatures and can be recognized if proper methods are used. S-Tools works by reducing the number of colors of the cover image to 32, but expands them over several color palette entries, if the palette is then sorted by luminance, blocks of colors appear to be the same, but actually have a one-bit variance. This type of variance pattern is extremely rare in a natural image. As mentioned earlier, instead of concentrating on steganographic algorithm, patterns in normal images can be implicit to determine the abnormalities in images that deviate those properties. One such method is to understand the order of statistics of natural images and then discover the alteration caused by the hidden message in these statistics.

S-Tools version 4 works in the Windows 95/NT operating system, but does not work with Windows 3.x or below. This version is very easy to use for someone with windows knowledge and its functions such as drag and drop. Multiple files can be hidden in one sound/picture and your data is compressed before being encrypted. S-Tools version 4 provides steganography to image files using BMP and GIF formats. Additionally, S-Tools version 4 allows for steganography to

applied to sound files with the WAV format. One module integrates both image and sound for ease of use. Another nice feature of S-Tools version 4 is the ability to continue working on your desktop without stopping workflow when you are performing multiple hide and reveal operations. S-Tools version 4 does not require a super computer to work; in fact, the program will fit on a floppy disk and ran fine on my Pentium II desktop.

Andy Brown authors S-Tools version 4, and it supports 24-bit image files and has an array of encryption routines with many options. Additionally, S-Tools version 4 has the option to compress the data to be hidden or stored in a raw mode. To resolve the problem of identical sets of data encrypting simultaneously, S-Tools version 4 inserts some random garbage on to the front of each data. The random garbage together with the data is then encrypted, using the pass phrase that is chosen, to generate the key.

S-Tools version 4 applies the LSB technique discussed earlier in hiding information. Instead of just dispersing the data to be concealed in linear fashion across the available bits, it uses a cryptographically strong pseudo-random number generator to determine the position of the next bit to use.

Using S-Tools version 4 is effortless if you understand Windows. First open up S-Tools version 4, then select the cover image file from windows file manager or windows explorer and drag it into the S-Tools window. Then select the type of encryption (between IDEA, DES, 3DES and MDC) and the password of your choice. S-Tools version 4 does not to waste your time by displaying the size of file that can be hidden in an opened cover file. Once the message is hidden the steganography image is displayed alongside the cover image for comparison. Then save the steganography image, and if "save" is chosen, the file will be saved under the name, "hidden". Either way, you have to make sure the file name ends in BMP or GIF. S-Tools version 4 looks at this part of the file name to decide whether to save the picture as a GIF or BMP file. One of the only limitations that I discovered with S-Tools version 4 is that you cannot use JPEG. Even so, S-Tools version 4 does provide you with a nice interface, a help feature, and a status line. The status line is helpful because it displays the largest message size that can be contained in an open file. Plus, you can toggle between the original file and the hidden file for comparison.

If you need to retrieve a message from an image file that S-Tools version 4 is displaying, you right-click on the image and opt for "Reveal" from the menu. Next, you will be prompted for the type of encryption algorithm used. The reveal task appears in the actions window for you to check on its progress. Lastly to open a file, you select it from the archive window and right-click on it. Then you will choose "Save as" from menu and the file can then be manipulated.

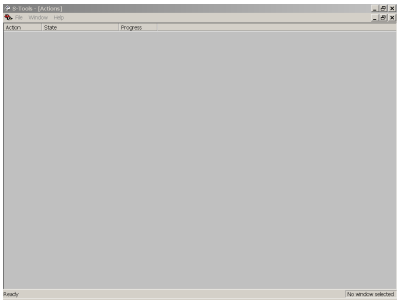

Figure 1

Figure 1 represents S-Tools desktop

Below are examples are two images using S-Tools, the first (Figure 1) is the original image file, the second (Figure 2) has an image of a map hidden utilizing steganography.

Figure 2

This is a picture of a puppy before applying S-Tools version 4

Figure 3

This is the same picture using S-Tools version 4

It is virtually impossible for someone to notice that the two images above are different just by looking at the images. However, any manipulation to the image initiates some amount of distortion and degradation in the image properties. The tools vary in their approaches for hiding information. Without knowing which tool

is used, identifying the hidden information may be very difficult. Steganalysis should be performed with the knowledge that tools produce steganographic images with characteristics that operate as signature for the method or tool utilized.

The detection of hidden messages in steganographic images is inspecting for obvious and repetitive patterns. This could lead to the identification or signature of a steganography tool or a hidden message. Distortions or patterns visible to the human eye are the simplest to become aware of. Identifying such patterns in images is to compare the initial images with the steganographic images and notice the visible differences. The small distortions in steganographic images may go unseen without the assistance of the comparison. Distortion can be introduced into an image, which might be similar to JPEG compression noise. This "noise" jumps out of the steganographic images when a comparison is perform with the original images. Comparisons with numerous images, patterns begin come into view as possible signatures to steganography tools. Some signatures may be exploited automatically to recognize the hidden messages and those tools used in embedding the messages. If the images are not available for comparison, the derived known signatures are enough to imply the existence of a message and identify the tool used to embed the message. Sometimes recurring, predictable patterns are not readily apparent even if distortion between the cover and steganographic images is noticeable.

Although it is not mandatory to use steganography tools, steganalysis can be performed in observing unusual or repetitive patterns, or through distorted noise, or the readability. However, with the most of the available tools, you are provided with output, which is essential for auditing and additional analysis purposes. Additionally tools are easy to obtain, often free or inexpensive, and very effortless to use. As mentioned above, S-Tools version 4 is simple to use, and does not require a high performance desktop, and it does not use very much space.

[11]Steganography tools are readily available which has law enforcement and others on alert for illegal misconduct. This fact should alert your company to guard against steganographic malicious intrusions. As technology is constantly advancing development into steganography will continue. The more that information is available on the Internet, the more the owners of the web sites need protect themselves from improper representation or worse.

One additionally thought if you were to protect your site by applying steganography with approved tools and adhering to your policies you can enhance your security. To do this we would use a tool such as S-Tools to add our company logo to images on our web site, and secure them with a password, and periodically check with integrity of the images with a scan. Additionally, if someone decided to thieve our images, they would have our logo behind them password, and the thief would incriminate themselves.

[12]In conclusion, your job is to keep in mind that steganography exists and is growing in popularity. As a security individual and primarily your work as a steganalyst can be performed with the knowledge and tools to assist your occupation. This paper has stated that steganography is difficult to detect and guard against; however, the risk can be highly reduced by providing a steganography policy to your company, and supplying approved tools to enhance your ability to protect your web site.

References:

[1]Johnson, N.F. and S. Jajodia. *Steganalysis of Images Created Using Current Steganography Software*, Information Hiding: Second International Workshop, 1998,
http://ise.gmu.edu/~njohnson/ihws98/jjgmu.html

[2]Krinn, Jeremy. "Introduction to Steganography." 26 Jun 2000.
http://www.sans.org/infosecFAQ/covertchannels/steganography.htm

[3]Yeuan-Kuen Lee and Ling-Hwei Chen. "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement"
http://debut.cis.nctu.edu.tw/~yklee/Personal/IS99-DataHiding.pdf

[4]Steganalysis: The Investigation of Hidden Information
Neil F. Johnson and Sushil Jajodia
September 1998
http://www.simovits.com/archive/it98jjgmu.pdf

[5]WetStone Technologies, Inc.
SMART Watch™
http://www.wetstonetech.com/smartwatch.html

[6]Christian Cachin. "An Information-Theoretic Model for Steganography" 2001

http://clue.eng.iastate.edu/~guan/course/paper/steganography/cachin01informationtheoretic.pdf

[7]The Stego Archive
http://www.stegoarchive.com/

[8] Krinn, Jeremy. "Steganography" viewed 12/16/2002

http://www.giac.org/practical/Jeremy_Krinn_GSEC.doc

[9] "Introduction to Digital Images" viewed 12/16/2002
http://www.people.virginia.edu/~cfr4r/imageintro.html

[10]Brown, Andrew: *S-Tools for Windows*, Shareware 1994. ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools4.zip (version 4)

[11]John Hally "Steganography: What's the Real Risk?" January 9, 2002 http://rr.sans.org/steg/risk.php

[12]What is Steganography?
Richard Lewis
February 10, 2001
http://rr.sans.org/steg/steganography3.php
Additional Resources:

Detecting Steganographic Content on the Internet
(Analysis by Neils Provos and Peter Honeyman at the University of Michigan)
http://www.citi.umich.edu/u/provos/stego

Petitcolas, Fabien a. p. "the information hiding homepage digital watermarking & steganography" 17 June 2002
http://www.stegoarchive.com/

Edmead, Mark T. "Introduction to steganography" 10 Apr 2002
http://searchwin2000.techtarget.com/tip/1,289483,sid1_gci815698,00.html

Ansuh, Francis "Steganography: Not Just a Tool For The Bad Guys"
http://www.giac.org/practical/Francis_Ansuh_GSEC.doc

"Steganography: High-Tech Hidden Messages" APR 30, 2002 ARTICLE ID: 1314
http://enterprisesecurity.symantec.com/article.cfm?articleid=1314&EID=0

Barratt, William. "Steganography Using Computer Images" 2002-10-28
http://www.tjhsst.edu/~wbarratt/techlab/proposal/

Mendell, Ronald. "Steganography - Electronic Spycraft" September 20, 2000
http://www.earthweb.com/article/0,,10456_624101,00.html

Mactaggart, Murdoch. "Introduction to cryptography, Part 1: The broad view" March 2001
http://www-106.ibm.com/developerworks/security/library/s-crypt01.html?dwzone=security

Reverser. "Reverser's Steganography (Starting Page)" September 1998
www.woodmann.com/fravia/stego.htm

Fighting Steganography Detection
Fabian Hansmann

January 4, 1997