Global Information Assurance Certification Paper

Steganography

Richard Lewis

What is Steganography?

Steganography, literally meaning *covered writing*, involves the hiding of data in another object. From the time of Herodotus in ancient Greece to the terrorist of today, the secret writing of steganography has been used to deny one's adversaries the knowledge of message traffic.

There are many tools that are freely available on the Web that will allow an individual to hide your data without your knowledge in an innocuous looking file. The only way that you would be able to detect this is if you happen to have a "golden" copy of the file in question. You would have to do a bit by a bit comparison of the file in question in order to detect the subterfuge. Now, the reasonable individual would concede, the chances of having a pristine copy of a file that you do not control are highly unlikely. So would not be a great leap of faith to understand that Steganography is one of the more serious threats to the data integrity and an organizations security posture today. It all boils down to trust, can you, do you, trust your employees.

Figure 1 Cover Image

As a security professional you are concerned with your organizations proprietary information being removed form your premises without your knowledge. Steganography provides the tools to do just that. Employee data, pricing data and rates, etc can be easily smuggled out right under your nose. Utilities that look for "dirty words" or key phrases are not going to be able to detect information that has been concealed.

How Steganography Works

Steganography works, in some cases, by using the lease significant bit (LSB) in a byte. By encoding the LSB of every byte in the file we are able to secrete data in an otherwise harmless file. In a bitmap file, as shown in figure 1 and figure 2, we can see some degradation of the image. In a

Figure 2 Stego Image

small file this is more apparent because of the higher ratio of modified bytes. (The larger the ratio of modified bytes in a file the more apparent the distortion.) If the file had been larger the same hidden file would have been barely noticeable, even when compared side by side with the original.

Baring the use of encryption, we can examine the file and tell whether information has been inserted into the file. Of course we would need a utility developed for that purpose, but given the power of today's desk top computers and the fact that the information is not encrypted we should have no problem in ascertaining the subterfuge.

When we are faced with the use of encryption and steganography together then out job is made much more difficult. The encrypted data should appear as background noise. Our simple scanner now can't find patterns scattered through the file. In order to combat a known encrypted steganography file we can alter the file in some way to make recovery of the message impossible. That can be accomplished by inserting our own message in the file. The damage done to the original message should render it unreadable. In the event the file in question is a stego image file we can crop or otherwise edit the file to render the message unrecoverable. Thus it is a simple matter to destroy a hidden message but detection and recovery are quite a different matter.

In a wave file the hidden data would appear as white, or random, noise. More than likely you would be unable to hear it; your dog might but not you. The casual observer would not find any evidence that data was being smuggled in or out of the facility.

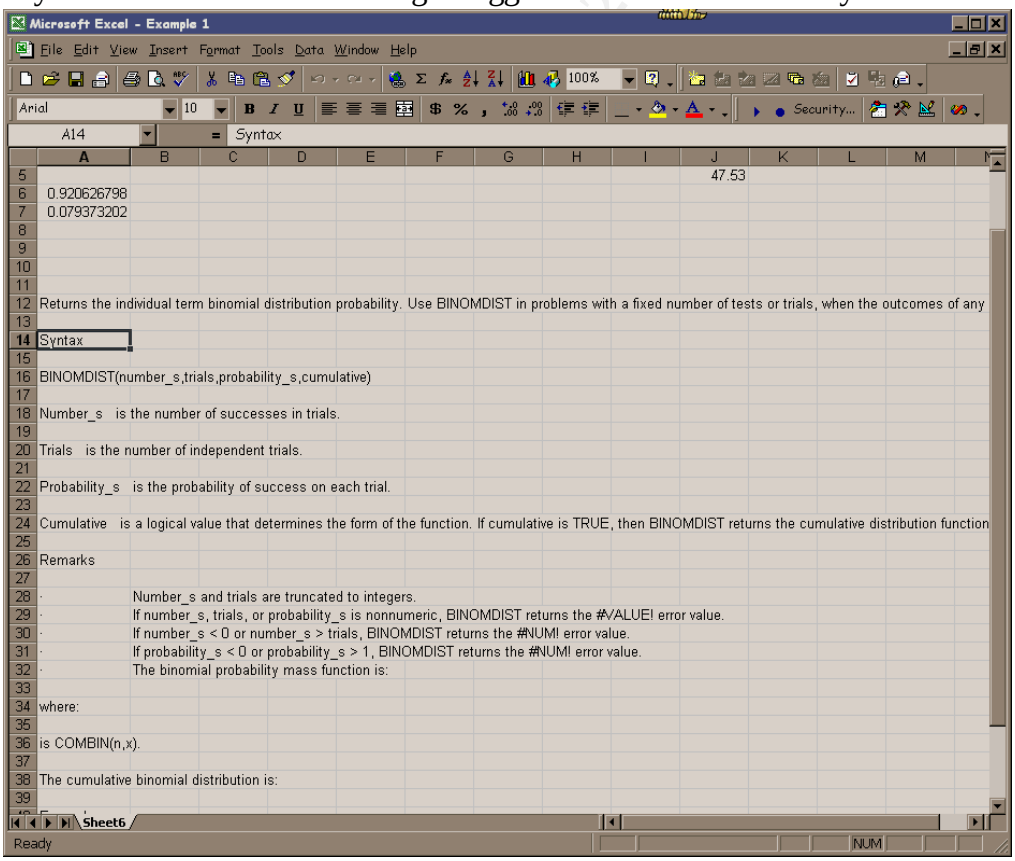

Figure 3 Stego Object

As you can see the first figure and the second figure appear almost identical if it were not for some image degradation the files would be identical. However, they are not. This is because the second image, through use of Steganography, contains a complete Excel spreadsheet. It is only because of the small size of the image file that we are able to see the degradation of the image. It is a good to note that the larger the image file the more data can be hidden there.

Vigilance Is The Key

I think now would be a good time to talk about bandwidth. As I have said, due to the small size if the cover image and the relatively large size of the Stego object, the Stego image has a noticeable amount of distortion present. It is easier to hide a small message in a large file, than a large file. One more concern is that of traffic flow security. If someone suddenly starts to take image and wave files out of your facility for no apparent reason then, you as a security professional, should become suspicious. To combat the threat you need to know the normal patterns and then look for changes in the norm. We always come back to know your system. I will expand that to, "Know your environment."

The S-Tools application is easy to use and the novice user can hide a large amount of data with little effort. The S-Tools application can be found at the following link. ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip

Once the application has been downloaded, installed, and started, you would just drag and drop a sound or picture file into the application's workspace. Now comes the fun part. Find the file that you want to hide. Simply drag the file over the picture and drop it. You will then see the passphrase GUI, see figure 4, enter your passphrase, select your encryption algorithm, and click on OK. That's all there is to it. Do not forget your passphrase.

Now if you think that you can use S-Tools to identify weather or not a file has hidden data in it, you are out of luck. Without the correct passphrase, you will not be able to tell. The data is encrypted so it will look like noise to the application if the correct passphrase is not entered.

Decoding or extracting the hidden file is also a simple process. The file that contains the hidden data is placed into the S-Tools work area. The mouse pointer is positioned over the file, and when you right click on the file you should select the reveal option. You will then see the passphrase GUI, see figure 4.you then enter your passphrase, twice, select your encryption algorithm, and click on OK. If you were successful the program will display the reviled archive window, see figure 6.

Summary

Steganography, literally meaning *covered writing*, involves the hiding of data in another object. Steganography provides the tools to do just that. Employee data, pricing data and rates, etc can be easily smuggled out right under your nose. Steganography has been with us since the

time of the ancient Greeks. Modern terrorists organizations use it to pass plans and information between cells by placing altered pictures in newsgroups on web sites and passing them in chat groups.

By encoding the LSB of every byte in the file we are able to secrete data in an otherwise harmless file. In a bitmap file, as shown in figure 1 and figure 2, we can see some degradation of the image. If the file had been larger the same hidden file would have been barely noticeable, even when compared side by side with the original.

Baring the use of encryption, we can examine the file and tell whether information has been inserted into the file. The encrypted data should appear as background noise. In order to combat a known encrypted steganography file we can alter the file in some way to make recovery of the message impossible. In the event the file in question is a stego image file we can crop or otherwise edit the file to render the message unrecoverable. In a wave file the hidden data would appear as white, or random, noise.

The ability to remove information undetected is a threat to the integrity of any organizations data. Protecting your organizations data requires hard work and diligence. Many tools are freely available on the web to secrete data and enable someone to smuggle data out of your facility. You must know your environment and become aware to changes in its patterns. Knowing that the threat exists is the first step on combating the problem.

Using encryption and steganography makes the job of detecting a hidden message much more difficult and more than likely would place it outside the ability of the average organization. If it is suspected that a file contains a hidden message, editing or cropping the image file or placing your own hidden message in the stego file can easily destroy the message.

To combat the threat you need to know the normal patterns and then look for changes in the norm. We always come back to know your system. I will expand that to, "Know your environment."

Steganography & Digital Watermarking Information Hiding

http://www.jjtc.com/stegdoc/stegdoc.html

Schneier, Bruce, *Secrets and Lies Digital Security in a Networked World*, John Wiley and Sons, Inc., New York, 2000, pp246

IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998
http://netsecurity.about.com/compute/netsecurity/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.cl.cam.ac.uk%2F%257Efapp2%2Fpapers%2Fjsac98-limsteg%2F

'Wavelet-based digital image watermarking', H-J. M. Wang, P.-C. Su, C.-C. J. Kuo, Optics Express, vol. 3 no. 12 pp. 491–496, 7 Dec. 1998 .
http://epubs.osa.org/oearchive/pdf/7081.pdf

Steganography Mailing List. Markus Kuhn -- 1995-07-03
http://www.thur.de/ulf/stegano/announce.html

Steganalysis of Images Created Using Current Steganography Software
Neil F. Johnson and Sushil Jajodia Center for Secure Information Systems, George Mason University
http://ise.gmu.edu/~njohnson/ihws98/jjgmu.html

An Introduction to Steganography, Duncan Sellars
http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html

Steganography,
http://www.tamos.com/privacy/steganoen.htm