GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Dan Henderson
GSEC Practical Assignment
Version 1.4b Option 1
03/10/2004

Steganography: Will your company use it or be used by it?

Abstract:
A steganalyst may use either steganography to pass information in a hidden manner, or steganalysis to detect hidden messages. This paper will give tips on how to use both steganography and steganalysis to protect your work environment. To accomplish this purpose we will discuss what steganography is, it's origins, and uses in today's society. Also steganalysis will be reviewed, with its history and uses in today's society. Finally we will discuss some possible uses for both of these tools in the corporate world of today.

Steganography can be used to allow your corporation to pass vital information within, or outside, of its structure, while still maintaining a high level of secrecy. This is often necessary in today's corporate world. If the information to be passed along has also been encrypted before being hidden, the odds of it being intercepted and private information leaked can become almost non-existent. On the other hand, steganography tools have become so easily obtained and easy to use, that you must be able to detect their use to prevent company secrets from being leaked intentionally. The loss of an earnings report or other vital data before the public announcement could not only be embarrassing but also devastating.

What are Steganography and Steganalysis?

Steganography is the art of passing a message or information in a way so that the very existence of it is not perceived. The theory of steganography is to be able to pass a hidden message without any suspicion of this happening; this goal is destroyed if suspicion is raised. Steganalysis is the art of finding those hidden messages, thereby making them worthless. These are of course very simple explanations of extremely complex arts, or as some would call them, technology.

History of Steganography

One early story relating the use of steganography tells of how the Greek tyrant Histiaeus tattooed a message on the shaved head of a slave. Once the slave's hair had grown long enough to cover the tattoo enough to fool the guards of king Darius, the slave was sent to the tyrant's son-in-law in another city. This all supposedly occurred in the 5th century BCE, and is one of the earliest known uses of steganography.[1]

[1] ALL nettools. Privacy Guide: Steganography.
http://www.all-nettools.com/privacy/stegano.htm (01-12-2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Another early story related in the Histories of Herodotus, tells how Demeratus wished to pass a hidden message to Sparta. He knew that Xerxes planned an invasion of Greece. At that time writing was done on wooden tablets covered with wax, Demeratus removed the wax from one such tablet and inscribed his message in the underlying wood, then covered the wood with a fresh coating of blank wax. Once again the guardians were fooled by the ruse.[2]

Even as late as WWII many secret messages were passed with very old techniques such as invisible inks made by using milk, urine, fruit juices or vinegar; all of which darken when heated. So often the real message was "between the lines". However, during WWII the Germans created a technological advance in steganography that still has many uses today, the microdot. The microdot allows large amounts of written data or drawings to be reduced to the size of a period in a sentence, or perhaps the dot over an i anywhere in a document.[3]

With the advent of computer technology and the Internet, the art / science of steganography has moved forward again. Many methods are available with the use of said technology, such as hiding the message in a text file by merely changing the font color to the same as the background, embedding the message within a sound file in such a manner that the sound is not altered. Or even as seen recently used among many terrorist organizations the embedding of a message within a picture file in such a way as to render it unchanged to the human eye.

History of Steganalysis

The history of steganalysis, as you may have guessed, is closely related to the history of steganography. When one advances, the other must also advance, to temporarily neutralize or surpass the other. In the early days it may have been as simple as teaching the guards to also check a person's scalp for messages. Or training the guards to more effectively search the objects being passed back and forth.

During WWII the use of steganography, and the suspicions created by it, became so prevalent that the "guards" could no longer keep up with the searching in an effective manner; so many rules, restrictions, and laws were passed to attempt to stem the flow of hidden messages. Today many of these fears seem almost silly. The US banned all children's drawings, knitting instructions, games of Correspondence Chess, and newspaper clippings from traveling through the country's mail. It also became illegal to order specific flowers to be delivered on a

---

[2] Johnson, Neil F. History and Steganography. http://www.jjtc.com/stegdoc/sec202.html (01-12-2004)

[3] ALL nettools. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm (01-12-2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

specific date. In both the US and Britain international flower orders were made illegal. In the USSR all international writings were screened for hidden messages.[4]

In the last couple of years steganography has been discovered to have been used by terrorist organizations to pass instructions to each other. Their messages have been hidden in mp3s and picture files, prompting the government of the United States to begin contemplating some very stringent laws pertaining to all forms of communication. It seems that no matter what time in history, steganography with its ability to hide messages, inspires distrust and fear.

You may notice that there is quite a similarity between the steganography / steganalysis and the virus / anti-virus relationship. It seems very similar to a race, one side comes up with an advance that is soon copied and used by the other. We are the "guards" of our respective corporations, and our job is to stop the passing of information from our company. Just like the guards of old, one way to stop the loss of information is to acquire more training. It is a constant process due to the fact that like the "anti-virus guards", the "security guards" are greatly outnumbered. Even the most conservative estimates show a huge disparity between the numbers of trained security personnel and the number of hackers, crackers, and thieves.

How can your company use Steganography?

There are almost as many uses for steganography as there are programs to make its use easier. Now we will discuss some of the ways in which your company could benefit from the correct use of this age old / modern concept.

Copyright protection is just one of the many uses for steganography, if your company publishes a great deal of written material, pictures, or even music files digitally the odds are that you are already interested in digital watermarking, or as it is also sometimes called, digital fingerprinting. Currently this form of steganography is fairly popular being used by many large corporations, unfortunately that also makes if vulnerable to those that wish to render it useless.

E-mail has become vital to the corporate world, and because of that fact many companies now scan all incoming and outgoing email for viruses and other things, but what if you did not want the email administrator to know exactly what was in the email being sent? Passing secret messages to a client or co-worker in seemingly innocuous emails is another use for this art. Many companies have a need to send information to a client that may in some cases be quite sensitive, such as a salesman confirming a new price or rebate that should not become know by the general public. Another such use would be a CFO sending as yet unreleased information to the CEO before a board or stockholder meeting.

[4] ALL nettools. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm (01-12-2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Even the company web page can be used to pass secret information in a simple manner. This may be a planned thing used by your company, or could be an unplanned thing used against your company. This information can be contained in images, videos, audio files, or even web page text.

Another use for steganography is in hiding files and directories on your network or even on an individual hard drives. This use of this skill can allow an IT person to create many safeguards on the network or individual drives to facilitate recovery or rebuild after a disaster.

Now lets examine some of these uses and how they can be implemented.

Digital Watermarking

Copyright protection through the use of Digital Watermarking is currently in use by many companies, especially those that use the Internet as a marketplace. One of the larger companies promoting and selling Digital Watermarking software is Digimarc. Digimarc promotes its products by making the following claims.

> Digital watermarking can confirm an identity, provide secure access to restricted areas or connect print content to a dynamic, multi-media environment with more possibilities than one could ever fit in a printed page, an audio file, a video or a digital image.[5] Digimarc. Digimarc Products. http://www.digimarc.com/products/default.asp (02-26-2004)

Similar products are currently used by many manufacturers of DVDs and CDs as one way of preventing the copying of their material. Firms that publish pictures and videos on the web, such as E-zines, use it to embed their watermark in the material in such a way that the human eye cannot see it but a computer can easily distinguish the marking. Making very tiny and subtle changes to the original digital data does this. The coding to prevent copying of such DVDs and CDs is built into many DVD and CD recorders. There are also companies that specialize in creating a database of your images and then use a form of web crawler to search the Internet, comparing images that the crawler finds against that database. In this manner they claim to be able to provide copyright protection to their customers.

Digital watermarking or digital fingerprinting is already in very widespread usage on the Internet with information available quite readily on the companies that specialize in it, as well as, how to contact them and use their products. Just be aware of the fact that it may be an excellent use of steganography to protect any and all proprietary images that may be posted on your company web site.

Email

Email has become one of the primary ways many companies communicate. It

[5] Digimarc. Digimarc Products. http://www.digimarc.com/products/default.asp (02-26-2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

has become so important to most companies that the thought of losing email, or having their email system crash, gives many corporate executives nightmares. Salesmen use the company email system to communicate with existing clients and prospective clients. Accountants no longer need to carry a huge stack of paperwork to another's office; they merely email it to them. Supervisors keep tabs on vacation requests, and upcoming meetings, all through email.

So how does steganography fit into this situation you may ask. The following situation might be one use of steganography for your corporation. The CEO is located in the home offices in Chicago, the CFO is located in another major office in Tucson, and the company is working on trying to obtain a government contract that could easily double the size of your work force, product output, and of course a sizable bonus for both of the executives mentioned. The CFO has to get vital numbers to the CEO by 10:00 am and it is now 9:00 am. Of course the CFO could always call the CEO on the phone, but the wrong ears might overhear that conversation. The CFO could send a fax, but would be required to stand at the fax machine to send it; and the CEO would have to stand at the fax machine to receive it, to maintain security. Of course that is a waste precious time for both persons. Luckily for these two executives, a plan was offered by one of the company security personnel to be used in just such a situation. The CFO uses a couple of pieces of software, that they have received a small amount of training with, to first encrypt the vital information and then embed that encrypted data into an mp3 file. Now an email is prepared and sent to the CEO with a predetermined subject line that indicates the attached file has hidden data. In this case the subject line could be something like: Here's a song to help make you happier today! In the body of the email is the line: I know things are tough there today but this song is really cheerful. The subject line tells the CEO that attached song has data embedded in it, and the last word in the body of the letter is the password to use when decrypting that data file. Now the time is 9:45 am and the CEO has not only gotten the email, but has also already removed the data file and decrypted it. The vital numbers are there and nobody is the wiser that they have been transmitted since the executive make it a point to exchange an mp3 file every now and then as a cover for just such occasions.

If the email administrator intercepts the email, he sees it as just another normal email. If a competitor, hacker, or thief intercepts the email from the Internet; it seems innocuous enough that it would draw little attention. Perhaps someone would be smart enough to suspect a hidden message. The encryption would delay their doing anything with the data, should they find it, until the data no longer needs to be kept secret. Remember, to find the data someone would need to first suspect that it is there and these executives had already established a pattern of exchanging mp3 files that would make suspicion unlikely.

Sound like the plot of a James Bond novel? Not really, the software is readily available on the Internet for free that can accomplish every step in our little scenario. Not only is it available, but also it is simple to use. Even the most

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

technologically challenged CEO or CFO would not find using such software much different from using email, word processing, or spreadsheet software. Instead of mp3 files picture files can be used for smaller data sets, it is all a matter of personal preference.

A competent security person can very easily put together a quick training session and burn the needed files to a CD ROM, arrange time with both executives, either by phone or online conference. Train the people, install the software, explain the importance of establishing a routine ahead of time, also explain a few of the possible legal implications, and look like a genius for thinking of the entire process before it is ever needed.

The software is more of a personal preference depending on your OS and networking environment, however, a couple of quick examples are Wincrypt 2.0 available as shareware at http://www.wincrypt.com/encryption/encryption.htm with support and instructions also available through the links on that page.[6] Wincrypt. Encryption. http://www.wincrypt.com/encryption/encryption.htm (02-26-04).
Also basic instructions for MP3Stego can be found at http://www.techtv.com/screensavers/answerstips/story/0,24330,3375638,00.html the download is available there as well.[7] TechTV. The Screen Savers. MP3 Steganography. http://www.techtv.com/screensavers/answerstips/story/0,24330,3375638,00.html (02-26-04).
Or for a fully GUI based answer try Steganography 1.60 is available at http://www.soft32.com/download_16049.html as a shareware program that can then be upgraded.[8] Soft32.com. Download Steganography 1.60 for free. http://www.soft32.com/download_16049.html (02-26-04).
After trying some of these, or other, tools; I believe that you too will agree that anyone can be taught to use them quickly and easily.

Hidden on the Network

Data, files, and even entire directories can be hidden on your company LAN. This may be something that you are doing already to one degree or another. It can be as simple a thing as having a buried file within a directory, burying a directory so deeply that most people would not bother to drill down to it, or using null

---

[6] Wincrypt. Encryption. http://www.wincrypt.com/encryption/encryption.htm (02-26-04)

[7] TechTV. The Screen Savers. MP3 Steganography. http://www.techtv.com/screensavers/answerstips/story/0,24330,3375638,00.html (02-26-04)

[8] Soft32.com. Download Steganography 1.60 for free. http://www.soft32.com/download_16049.html (02-26-04)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

characters in the name. As in most cases, the more simple an implementation is, the easier it can be defeated by a dedicated hacker / cracker. In many of the cases of hidden network files and directories, they are there to help for cases of disaster recovery.

Once again there are programs that are readily available, many coming with your OS or setup files, that can accomplish hiding files or directories. Depending on your OS, it may even be an integral part of the operating system.

It is VITAL that your company use something to protect sensitive and copyrighted materials both inside and outside your company. The Internet made invasion of a corporate LANs a daily event, and every security person knows the problem is only escalating. Steganography can be an effective tool / weapon in your security arsenal, and can provide at least a measure of protection. But to be protected, your system has to be in place BEFORE an attack.

How can your company use Steganalysis?

Detecting hidden information defeats the goal of steganography, imperceptibility. Many tools exist that can help detect hidden data in various types of files, and they should by used, not only to detect data but also to test your system and how well your chosen method of steganography protects your company. Much as a network administrator tests the strength of passwords used on the LAN, the methods of hiding data must continually be tested, tweaked and improved.[9]

Johnson, Neil F. and Jajodia, Sushil. Steganalysys: The Investigation of Hidden Information. http://www.simovits.com/archive/it98jjgmu.pdf (03-08-04)

Image Archival

Having an archive of the images used by your company web pages stored with an MD5 hash-marking system will enable you to determine if the images have been altered on the website or within the company. Using a digital watermarking system, a well-tested system, can also help prevent your images from being used against you. Or your corporation may find it more to its advantage to hire a company to archive and hash mark, test, and then patrol the Internet for piracy of your company's proprietary images.

Email

Testing of incoming and outgoing email should also be one of your methods of "Guardianship". In our earlier example steganography was used to benefit the company, with the knowledge and help of the security personnel, and was found to be quite a useful tool that enabled executives a quick effective manner of data transmission. But you never can tell when even a trusted employee may become disgruntled or coerced by another corporation, and therefore begin giving out company secrets; insider attacks are still the most expensive type that companies must deal with.

---

[9]Johnson, Neil F. and Jajodia, Sushil. Steganalysys: The Investigation of Hidden Information. http://www.simovits.com/archive/it98jjgmu.pdf (03-08-04)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In 2002 Computerworld magazine carried an article that told of an engineering firm that had been damaged through the use of steganography and email.[10] Radcliff, Deborah. Computerworld. Steganography: Hidden Data. http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html (03/08/04)

Email is so vital and so widely used that it has become easy to let some things slide in the interest of increasing speed and hopefully productivity. However, the use of steganography has only spread more and become easier to use without having actual knowledge of the mathematics involved. All email must be scanned and checked if an organization wishes to have true security.

Hidden files

Hidden files or directories are sometimes difficult to detect, but sometimes as easily detected as running a Windows file search. Other times the tools used to locate such files and directories become quite complicated, but are well worth the time and expense involved in becoming familiar with them. Never forget that there are many utilities out there freely available that will overwrite an empty, or seemingly empty, portion of a hard drive, thereby destroying hidden information completely

Policies and Procedures

Few persons enjoy having to write or enforce policy and procedures; however, to the security personnel it is a core function, especially when dealing with a tool as potentially damaging or useful as steganography. Without procedure you cannot legally enforce policy, period.

Corporate network users commonly will download and play with things they should not, and invariably cause some type of problem on the network or their own PC. I have heard more than one network administrator comment on how secure their network could be if they did not have to let the other employees use it.

This leads to many legal questions, some of which are still unanswered and some are yet to be asked. A good security person should make it a point to stay current on some of the legal issues that we are required to deal with on a daily basis. However, without written policies in place and documented procedures on how to enforce them, all the work you do to protect your company will be absolutely useless.

Do not forget that in your policies and procedures it is important to establish exactly what the limitations are for the security personnel themselves. Then

[10] Radcliff, Deborah. Computerworld. Steganography: Hidden Data. http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html (03/08/04)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

make sure that all the personnel know those limitations and adhere to them. Also it is important that all employees know that their computer, email, directories and files can and will be checked for appropriate content and security purposes.

Conclusion

This paper first gave a brief definition of steganography and steganalysis, the definition as it was used in this paper. Other definitions and explanations do exist for this varied and wide-ranging art. A very brief history of both steganography and steganalysis were given including some small examples. Also some tips were discussed for possible uses and abuses of these arts. Please remember that the uses for steganography, and therefore steganalysis, are only restricted by our imaginations and the current state of technology.

From there we moved on to a very limited number of the current uses for steganography and steganalysis. Some other possible uses were also examined. Policy and procedure were discussed, but could never be stressed enough in any article. Hopefully you now realize some of the benefits that your group, company or organization could gain through the use of these tools. Once again the question must be asked, will your company use steganography or be used by it? Only you can choose.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

[1] ALL nettools. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm (01-12-2004)

[2] Johnson, Neil F. History and Steganography. http://www.jjtc.com/stegdoc/sec202.html (01-12-2004)

[3] ALL nettools. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm (01-12-2004)

[4] ALL nettools. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm (01-12-2004)

[5] Digimarc. Digimarc Products. http://www.digimarc.com/products/default.asp (02-26-2004)

[6] Wincrypt. Encryption. http://www.wincrypt.com/encryption/encryption.htm (02-26-04)

[7] TechTV. The Screen Savers. MP3 Steganography. http://www.techtv.com/screensavers/answerstips/story/0,24330,3375638,00.html (02-26-04)

[8] Soft32.com. Download Steganography 1.60 for free. http://www.soft32.com/download_16049.html (02-26-04)

[9] Johnson, Neil F. and Jajodia, Sushil. Steganalysys: The Investigation of Hidden Information. http://www.simovits.com/archive/it98jjgmu.pdf (03-08-04)

[10] Radcliff, Deborah. Computerworld. Steganography: Hidden Data. http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html (03/08/04)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS