Practical Assignment

December 1, 2001

Prepared For:
SANS Security Essentials
GSEC Practical Assignment
Version 1.2f

Prepared By:
Nathan Delane

Table Of Contents

Purpose...1
Introduction 1
Encryption..1
Steganography 3
Digital Watermarking 5
Conclusion 6
Bibliographies...8
Software Links..8

Purpose

The purpose of this paper is to provide the reader with an overview of three aspects of Information Hiding and their current and future relation to information security. Though these issues are not always a major topic of discussion, they are still of vital importance, and they are quickly becoming the focus of newfound discussions.

Introduction

When delving into the realm of Information Security there are and will continue to be an abundant amount of topics to be discussed. Trying to protect systems and information from compromise is a never-ending job. While many individuals, corporations, and government agencies are consistently worried about the network and website attacks, viruses, and constant system administration, lurking in the background are other issues that do not receive as much attention but are still important topics that should not be forgotten. The topics that I am referring to are all related to Information Hiding; it doesn't sound like it's a major issue, but is it?

Make no mistake about it, every aspect of information security is part of a ongoing "***war***" (A concerted effort or campaign to combat or put an end to something considered injurious). It has become an information war, and protecting that information has taken on a new precedence since the issues are reaching closer to home. Some of the issues that I am referring to are theft of proprietary information such as credit card numbers, the terrorist attacks of Sept.11, 2001, and the illegal use of information such as the unauthorized download of digital media from MP3 sharing sites such as Napster. If you read into the definition of war and apply it to these scenarios, don't they all seem to fit the mold? Though all of these situations are different, they're all relevant to the area of information security. Everyone from the home-users to government agencies are using the vast resources of the Internet to communicate and transmit data in what they hope to be a secure environment, but just as resources are used for good purposes, they are also being used for the opposite. In researching the area of Info Hiding, I found three areas that seem to be relevant pieces to the puzzle: encryption, steganography, and digital watermarking. Each area has a different focus, and therefore has its own uses, advantages, and disadvantages; and this is what the paper will focus on.

Encryption

What is encryption?
It is the process of converting messages, information, or data that is in a plain text form into a form unreadable by anyone except an intended recipient. This is done to prevent valuable or proprietary information from being read by those that it is not intended for. This technique has been around for a long time and can dated back to the times of the Romans and Julius Caeser, in which a cipher was used called the Caeser cipher. Caeser thought that some people may find his jokes offensive and he wanted to make sure that they were protected, so he used a technique that rotated the characters forward a certain number of times. The technique rotated the characters forward 3 times, so for example, the word "PIG" would become "SLJ". Though this may seem like a very primitive method, it is still in use today on Usenet but the rotation number has changed. Encryption algorithms are used to transform the messages or information into ciphertext

(the encrypted message), and upon someone receiving the message, a decryption technique must be used to transform the message back to its original text form. Encryption has been in use for thousands of years, and methodologies of today are under constant scrutiny and revision to try to ensure that the algorithms are unbreakable. Just as individuals are out there trying to develop algorithms, others are trying to crack them; it's a never-ending cycle. There are several cryptographic algorithms (ciphers) in use today including DES, Triple DES, RSA, and AES, just to name a few. Each algorithm has a different formula and different method of encryption. So why not just use one for every situation? Each situation is unique and may not require the same degree of protection as the next.

How is encryption used?
Encryption is used in daily processes to protect information as it is passed back and forth between individuals, companies, and government organizations. It provides those people with a sense of privacy and protection, but is it enough? Everyday, technology makes another advancement forward, and on-line communications and transactions continue to thrive, but are we placing ourselves at even greater risk of releasing valuable information despite all the security measures we try to instill? Sure, we can use the triad of firewalls, intrusion detection, and log monitors, but if these security measures are surpassed, is our data still openly available to the hackers or thieves preying on our systems? Is it enough to just encypt the information traversing the web and networks? If we were to follow in line with the three major security objectives of confidentiality, integrity, and availability, it would make sense to go the extra step further and encrypt all data that we want to remain secure, whether it is to be transmitted to someone else or remain on the individual system. With so much information being passed around and computers becoming so much a part of the daily routine a lot of people seem to forget that there is always someone out there looking to intercept data. While some may not find something as important information, it may actually be just what an intruder is looking for. Encrypting the data would give an additional layer of security in that even if hackers find the encrypted data, they don't know what it is, and have to take the time to decrypt it, if they can. A technique as simple as this could save an individual or corporation a lot of headaches from the loss of data, which can also equate to the loss of money.

Public-key and secret-key cryptography can be used for encryption and each can have advantages and disadvantages. Below is a short description of each, but individual users would have to decide which method is best for the situation they face. In the eyes of many, a combination of public and secret-key cryptography is best so that users can benefit from the public-keys security advantages and the secret-keys speed.

Advantages/Disadvantages
Public-key (asymmetric: uses 2 keys): The public-keys principle advantage is related to security and convenience in that it is never necessary to transmit or reveal the private key to another party. Since the responsibility of protecting the private key is placed on the individual user, the public-key systems have the advantage of providing digital signatures that cannot be repudiated. One of the biggest drawbacks to public-key cyrtography is the speed; it is significantly slower than secret-key encryption techniques. It may also be possible for an attacker to impersonate anyone they choose by obtaining a public-key certificate on the system that's been compromised and binding a key to name of a user the attacker chooses.

Secret-key (symmetric: uses 1 key): The biggest advantage pertaining to secret-key cryptography is speed, but there are disadvantages of using this method as well. Since encryption and decryption are performed using the same key in a secret-key system it is necessary to transmit the secret-key, but this provides the potential for the key to be intercepted during transmission. Since it is necessary to share some sort of secret for authentication in this system, the receiver of a message can claim that the secret was compromised and repudiate the message. Even though public-key systems would seem to be more advantageous, this is not always true. Secret-key cryptography is suitable for certain situations. For example, in environments where users can meet face-to-face in private to exchange secret keys, or where one individual controls and manages all of the keys, it probably isn't necessary to use public-key encryption. Single-user environments are also a suitable area for using secret-key encryption.

Overall any type of encryption is better than none, whether it be public or secret-key. Though it may be an extra step in the security process and require additional time, users need to ask themselves, "Is it worth it?" If the extra time to encrypt the data were compared to the potential loss if your system were compromised and proprietary information were lost or stolen, would it be more beneficial to leave the information open or encrypt it? The answer seems obvious.

Steganography

What is steganography?
It is the art of hiding information or messages in ways that circumvent detection. The object is to convey information or messages to another party in a form that hides the very existence of the message in case the message were intercepted by another person. In today's digital era, these messages can be hidden in graphics, audio, video, or text files, but the most common is hiding information in digital images.

Just as encryption has been around since ancient times, so has steganography. The meaning of this word comes from the combination of Greek words *stegano* and *graphy*, which equates to "covered-writing" when combined. This practice has been used throughout history and can be traced back to ancient Greece. A couple methods that can be attributed to use by the Greeks was using wax-covered tablets and tattooing messages on shaved heads. The first method allowed a person to scrape the wax off of the tablet, apply their message to the wood underneath, and then recover the tablet with wax so that the message would remain hidden until the wax was removed again. The second method was to shave the head bald, tattoo the message or image onto the skin, and allow the hair to grow back. This would allow the message to remain unnoticed until the head was shaved again.

A couple other techniques can be place in more recent times of World War I and II. The first technique was used by the Germans in World War I, and followed a concept of microdots. They would take a message or image and photograph it and reduce it to the size of a period or a dot on the letter 'j'. Once the reduction was made, it could place in any written material and carried around inconspicuously by spies. This allowed for a very secure method of hiding information. In World War II, invisible inks were a common way of hiding information. Any type of letter could have imbedded invisible messages written on them without being seen by the human eye.

While these methods were effective during their times, things have evolved in today's digital age and become a little more advanced.

How is steganography used?
While other topics always seem to draw much more attention in the information security field, steganography has become a much hotter issue following the events that occurred on Sept. 11, 2001. While this form of information hiding may not seem to be a valuable tool for the average user, place yourself in the shoes of someone who has something to hide, and you may come to a different conclusion. When dealing with steganography, a picture may literally be worth a thousand words, but the frightening thought is that you may never know it! Take this statement and give it a thought, "All warfare is based on deception."(2) Does this sound like a scenario that can be applied to recent incidents? It is definitely a valid issue in the present and future of the information war. Not only do we have to worry about things we can see, but we also have to be cognizant of the things we can't see. In this ongoing information war there will always be the

In steganography two files are necessary to conceal the information that is desired to be hidden. The first file is the cover image and can be viewed as the container that will hold the information to be hidden. The second file is the information that is to be hidden. This information must be embedded in the cover image using one of the steganography tools and techniques. The hidden message can range from plain text to other images, and a stego-key (a type of password) can also be incorporated to hide the message and decode it at a later time. There are multiple tools available for operating systems ranging from Windows to UNIX; some of these tools are free, while others are available for purchase. If you would like to obtain or review some of the tools follow this link http://members.tripod.com/steganography/stego/software.html.

There are different methods for hiding information in digital images including least significant bit insertion and algorithms and transformations. Here is a brief overview of each approach:

Note: It is good to remember that most steganography software recommends using either the 24-bit images (BMP file) or 8-bit images (GIF file), as JPEG images are not supported or recommended.

Least significant bit insertion – This is the most common and simple approach to concealing information in a cover image. How does this work? The cover image is normally a 24-bit or 8-bit image, and the LSB (also referred to as the noise), or rightmost bit (ie. 11101000) has the data embedded into it by replacing it with a single bit of the data that is to be hidden. It is possible to replace the least and second least bit in 24-bit images without the eye being able to distinguish the change in the cover image. In using 8-bit images for cover images it is particularly essential to chose the right image, as 8-bits do not allow the same depth as the 24-bit, and hiding certain information will make a visible change to the cover image. The change occurs because the pointers to the color palette positions are modified and this can cause colors to be swapped and so forth.

Algorithms and Transformations – In this method, JPEG stego-images are created by using a JPEG algorithm to combine a cover image and a message to be hidden. In addition to using this algorithm, there are several other types of software that apply different techniques. For example, information can be spread and scattered throughout images using techniques such as Patchwork, which use redundant pattern encoding (spread spectrum methods) to thoroughly hide the information. Then there are other techniques that encrypt and scatter the data to be hidden throughout the host image. By encrypting and scattering the data, even if the hidden message bits can be extracted, they are useless without also having the stego-key and algorithm to decipher them.

Advantages/Disadvantages

While steganography tools would seem more useful for deceitful purposes than for good, that doesn't always have to be the case. For example, consider a scenario of a businessman who routinely carries a personal laptop, and on that laptop is sensitive corporate data. If steganography tools were used to hide the sensitive data in documents or images that seemed unimportant or ordinary, the data would be more protected should the laptop be stolen; since laptops are a high theft item, this is not a far fetched scenario. To further secure the data, the businessman could use a stego-tool that combines encryption; in which case the data would be unreadable without the secret-key should it be found. While steganograhpy will not be advantageous in every situation there are cases for using such a tool.

One of the main areas of concern in the security world today is preventing other possible terrorist activities. It seems that terrorists and other unlawful individuals and organizations are using this form of information hiding (steganography) as means to transmit data or communicate with each other in a covert manner. According to nameless "U.S. officials and experts" and "U.S. and foreign officials," terrorist groups are "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites."(4) Steganography allows these types of people to place their hidden communications in a image or message then place that message in a central location (drop point), thereby allowing others to access the information without ever having to make face-to-face or verbal contact with the one who posted the message. What better means of communication could a terrorist use in such a stealthy manner? To make matters worse, an unwitting host of the site or domain could be running a central point of contact for terrorists or other groups without ever knowing it. It is still hard to tell if an image has been manipulated with steganography software, and even harder to track where the images may be, and who put them there. There are millions of people surfing the Internet daily, uploading and downloading information and images, and posting messages; so think about this, that next graphic you download could contain the next terrorist plot, but would you know it?

Digital Watermarking

What is watermarking?

Digital watermarking is the process of embedding or inserting bits of information within a digital file, and while it can also be seen as a form of steganography, it is useful in its own right. Watermarking can be performed on images, audio, or video files and normally the copyright information (author, rights, identification.) is the information that is inserted. The watermarks are dispersed into the files as noise, and are normally spread throughout the entire file to prevent the watermark from being altered even if portions of the file are manipulated. The originator's profile information is stored in registration databases, and these databases keep track of the various identification numbers of different watermarks and their related originator's information. This form of information hiding has taken on a new importance since it so easy to steal, copy, and redistribute all forms of media on the Internet whether it is copyrighted or not. Even though this is an illegal practice, it is still a daily occurrence. Watermarking copyright information is seen as a possible solution to keep content users from possible theft and redistribution.

How is watermarking used?
Watermarking is being used to provide indication of ownership, the rights and restriction of media, and its conditions of use. This is an attempt to protect the rights of the originator of the media in case of illegal copying and redistribution. This will provide the originator with verifying evidence of ownership should it become necessary. Watermarking can also be used as a means for advertising.

There have been numerous proposals for requirements pertaining to the use of watermarks. Here are just a few:

-it should be difficult to erase the watermark as well as being difficult to add a new watermark
-the watermark should be subtle and not disturb the original use of the object
-the watermark should not be visible so that if illegal copying occurs the thief is unaware that there is evidence of his/her actions.

Advantages/Disadvantages
A watermark does provide the advantage of embedding copyright material and allowing an organization or individual to show its ownership for some sort of digital media.

Though there is an assortment of watermarking software on the market, they don't all perform in the same capacity. Some watermarks are easily removed by modifying or manipulating certain parts of the file, and some watermarks can even be forged. Any sort of major manipulation of files will usually invalidate a watermark. Depending on the type of media and encoding formats being used, different watermarking techniques may be necessary. Even if a piece of media does contain a watermark it does not necessarily show true ownership, this requires the participation of a third party. Just as encryption and steganography provide that additional layer of security, so to does watermarking. Each technique has its own uses, but they are all part of the information security tools, and if they can benefit an individual or organization, then they are serving their purpose.

Conclusion

Hopefully, the overview of the information hiding techniques provides some answers as well as provoking some questions. When there is so much information and technology, it is only logical that many problems will come along with it, it's all part of evolution. Just think, it wasn't that long ago that the Internet came upon the scene, and now we are in the digital age. Now millions of people enjoy the vast resources and abilities that the Internet and related tools and technologies provide, but those tools are not limited in who uses them and how. The same tools that provide corporations and government a way to have secured transmissions work the same for anyone else. We have to be vigilant in staying current with the issues at hand, and with so much technology available to us, that seems hard to do, but the recent attacks have changed the world's conception of security in every manner. The majority of people who enjoy the luxuries of the Internet may not have imagined that hidden messages outlining terrorist activities and plots could be so inconspicuously placed on any website. Terrorists no longer have to meet face-to-face to plot disastrous events, they don't even have to leave the computers in their apartment. There are no guidelines or restrictions to stop criminals from using the tools for deviant acts, and that's the problem. While debates are likely to proceed about the use of these tools, the war continues, but can we determine that taking these tools away from everyone would put a stop to their use; probably not. It has already been noted that terrorists like Osama Bin Laden is using encryption and steganography tools as a means to communicate with other terrorist cells, but where? And who posts and reads the messages? Those are the million dollar questions, and the problems that are being faced because these tools are available to both sides. Even if the tools weren't available to the public, terrorist have mathematicians and scientists that are at their disposal.

We also have to be aware that steganography and encryption tools can be used by internal personnel in corporation and government, and they are another type of threat that we face. While the issues of terrorists are a harder problem to deal with, some common sense approaches can be taken to deal with internal problems. For instance, a good first step is making sure no steganography or encryption software resides on machines unless it is part of the person's job. Another measure that can be taken is to do some sort of pattern matching analysis and look for large images and check to see if the images match the context of the message being sent, or are the same images being sent multiple times with a differentiation in size. It all boils down to being aware of your environment!

And while other luxuries such as MP3 downloading and copying images for personal use may seem like an inherited benefit of using the Internet, they are not. Although it is common, and hundreds of thousands of people are using sites similar to Napster daily to acquire everything from music to software, the push is on to put an end to such providers. Creators and originators of this distributed material are hoping that research in the areas of digital watermarks and fingerprinting may provide some solutions, but how far are they willing to go to protect their media, and how far will others go to get it for free? While corporations are spending money to protect their data, hackers and hobbyists use idle time to accept the challenge of trying to defeat the defenses, but this will always be the case. As we know, information security has been around for a long time, and it is not going away, so we must do our part and try to figure out the puzzle because as we've seen…the war is continuing!

Bibliographies

1. Digital Watermarking
   URL: http://condor.depaul.edu/~elliott/ds/projects/Spring98/BlueGroup/watermark.html
2. Johnson, Neil F., Jojodia, Sushil. "Steganography & Digital Watermarking Information Hiding" URL: http://www.jjtc.com/pub/r2026.pdf
3. Katz, John. "The Rise of Steganography"
   URL: http://slashdot.org/features/01/05/03/2043244.shtml
4. Levy, Steven. "Did Encryption Empower These Terrorists"
   URL: http://www.msnbc.com/news/627390.asp?0si=-&cp1=1
5. Marshall, Paul., Powers, Larry. ""Hiding in Plain Sight, Terrorists Use Steganography and Strike Again" URL: http://www.newmediamusic.com/articles/NM01090145.html
6. Marshall, Paul., Powers, Larry. """Steganography" As aTheWay to Make Music Downloads Secure" URL: http://www.newmediamusic.com/articles/NM01030321.html
7. Scheiei, Bruce. "Crypto-Gram Newsletter", Sept. 30, 2001.
   URL: http://www.counterpane.com/crypto-gram-0109a.html
8. Shaw, Sandy. "Overview of Watermarks, Fingerprints, and Digital Signatures"
   URL: http://www.jtap.ac.uk/reports/htm/jtap-034.html#7
9. Tzu, Sun. "The Art of War" translated by Lionel Giles, M.A. (1910)
   URL: http://www.chinapage.com/sunzi-e.html

Software Links

1. Steganography Software
   http://members.tripod.com/steganography/stego/software.html
2. Steganography Software
   http://www.sevenlocks.com/SWSteganography.htm
3. Watermarking Tools and Links
   http://www.stegoarchive.com/