Global Information Assurance Certification Paper

John Hally
GSEC Practical Requirements v.1.2f

Steganography: What's the real risk?

Introduction:

Since September 11, 2001, government officials have sought to change federal and state surveillance laws in order to allow the Federal Bureau of Investigations and the Central Intelligence Agency the ability to monitor suspected terrorist communications inside the United States. Typical monitoring practices include phone tapping, interception of mail, and both video and audio surveillance. With the age of the Internet, a whole host of new ways to communicate has arisen. Now law enforcement officials have to deal with communication as simple as email and as complex as triple-DES encrypted data streams. With all of the different types of data that would need to be analyzed, the key would be to analyze the important data. It's common knowledge that if you're looking to keep information private, encryption is the obvious choice. The different types of encryption are also known to have specific detectable signatures when analyzed. Steganography is a means to pass hidden messages in seemingly harmless documents, pictures, and video and sound files. With the amount of information that would need to be processed, its easy to see how certain data may get overlooked, like Spam email messages, web browsing to arbitrary sites, and the like. This is exactly where covert communications may be taking place with the help of steganography. USA Today reported that terrorists are using steganography to hide their communications from law enforcement.[1] The first Osama Bin Laden video was kept off of network television for fear of secret messages being relayed to potential terrorists still in the United States. How hard would it be for an image or email be propagated out to thousands of people containing information without being detected by anyone other than someone actively scanning for it? The answer is very easy, and it could be very nearly untraceable.

Steganography: What is it?

The definition of Steganography is literally, covered writing[2]. The idea behind Steganography is to pass a hidden message within another seemingly harmless message so that no one determines that hidden communication is taking place. Cryptography, on the other hand, relies on the cipher to protect the message from being decoded regardless if the message is detected and intercepted. Different types of Steganography have been used throughout the ages. One of the first documented uses of steganography was back in ancient Greece. Text was commonly written on tablets covered with wax. Demeratus wanted to notify Sparta that Xerxes intended to invade Greece. To inform Sparta, he

[1] Niels Provos, Peter Honeyman,Detecting Steganographic Content on the Internet, Section 1, http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

[2]Dr Anthony Ho, Internet Business 99, Singapore, 24th June 1998, Page 2, http://www.datamark-tech.com/publications/steganography.pdf

inscribed messages on the underlying wood and recovered the tablets with wax so that the sentries would not notice anything unusual during inspection.[3] Today, with new technologies and the abundance of processing power available at relatively cheap cost, there have been many tools developed to hide messages in email, embed data in images, and pass information through video and sound.

Tools of the Trade:

SpamMimmic[4]

SpamMimmic is a process that the people over at http://spammimmic.com/ have developed to encode and decode email messages to be disguised as spam. Considering the amount of Spam that is sent around the internet, and also considering that most people either filter it at the mail server or just delete it, its really an ingenious idea. This really makes security through obscurity a reality. Let's say some terrorist group wants to coordinate some type of action to its followers in the United States. Using an anonymous email application, or a hacked server for that matter, the message could be sent to a huge mailing list just as any other Spam is done. The people who are expecting the mail could take the Spam-encoded message, and simply decode it. Why not just use PGP or some other encryption software? Mainly because if you are afraid of being monitored, encryption leaves an obvious trail and is easily detected. If you're monitoring traffic, a simple Spam message could easily slip through undetected as it has the form of plain ordinary text. Here's an example using spammimic's site to encode the message:

Gentlemen, the chair is against the wall. John has a long mustache. Thank you.

This message encodes into:

> Dear Friend , Your email address has been submitted to us indicating your interest in our newsletter . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1623 ; Title 3 ; Section 301 . This is a ligitimate business proposal ! Why work for somebody else when you can become rich as few as 97 WEEKS . Have you ever noticed people will do almost anything to avoid mailing their bills & nearly every commercial on television has a .com on in it ! Well, now is your chance to capitalize on this . WE will help YOU process your orders within seconds plus SELL MORE . You are guaranteed to succeed because we take all the risk ! But don't believe us. Prof Jones who resides in Washington tried us and says "I was skeptical but it worked for me" ! We assure you that we operate within all applicable laws ! You will blame yourself forever if you don't order now. Sign up a friend and you'll get a discount of 20%. Thank-you for your serious consideration of our offer! Dear Web surfer ; Especially for you - this breath-taking info . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1626, Title 9 ; Section 305 ! This is different than anything else you've seen . Why work for somebody else when you can become rich as few as 43 MONTHS . Have you ever noticed how many people you know are on the Internet and more people than ever are surfing the web . Well, now is your chance to capitalize on this ! WE will help YOU deliver goods right to the customer's doorstep plus decrease perceived waiting time by 170% . You can begin at absolutely no cost to you ! But don't believe us . Prof Anderson of California tried us and says "My only problem now is where to park all my cars"! We are licensed to operate in all states . For the sake

[3] Niel F. Johnson, Steganography, http://www.jtc.com/stegdoc/stegdoc.html, Section 2.2
[4] http://www.spammimic.com/

of your family order now . Sign up a friend and you'll get a discount of 30% ! Thank-you for your serious consideration of our offer . Dear Salaryman , This letter was specially selected to be sent to you . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1619 , Title 3 ; Section 302 . This is a ligitimate business proposal! Why work for somebody else when you can become rich as few as 63 days . Have you ever noticed how long the line-ups are at bank machines & people love convenience. Well, now is your chance to capitalize on this ! We will help you process your orders within seconds plus turn your business into an E-BUSINESS ! You are guaranteed to succeed because we take all the risk! But don't believe us . Prof Ames of California tried us and says "I've been poor and I've been rich - rich is better" . We assure you that we operate within all applicable laws ! You have no reason not to act now! Sign up a friend and you'll get a discount of 30%. Cheers ! Dear E-Commerce professional , This letter was specially selected to be sent to you ! If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our database ! This mail is being sent in compliance with Senate bill 1816 ; Title 5 , Section 308 ! THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich inside 58 months ! Have you ever noticed nobody is getting any younger and people love convenience . Well, now is your chance to capitalize on this ! We will help you turn your business into an E-BUSINESS and SELL MORE. You can begin at absolutely no cost to you . But don't believe us . Mrs Simpson of Arizona tried us and says "My only problem now is where to park all my cars" ! We are licensed to operate in all states. DO NOT DELAY - order today . Sign up a friend and your friend will be rich too . Cheers . Dear Friend , This letter was specially selected to be sent to you . This is a one time mailing there is no need to request removal if you won't want any more ! This mail is being sent in compliance with Senate bill 1619 ; Title 7 ; Section 306 . This is different than anything else you've seen . Why work for somebody else when you can become rich inside 66 MONTHS ! Have you ever noticed nobody is getting any younger and most everyone has a cellphone . Well, now is your chance to capitalize on this . WE will help YOU process your orders within seconds and turn your business into an E-BUSINESS ! You can begin at absolutely no cost to you. But don't believe us . Mr Simpson who resides in Washington tried us and says "Now I'm rich, Rich, RICH" . This offer is 100% legal . We beseech you - act now . Sign up a friend and you'll get a discount of 60% ! God Bless. Dear Professional , This letter was specially selected to be sent to you ! If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our mailing list . This mail is being sent in compliance with Senate bill 1623 ; Title 8 , Section 307 . This is a ligitimate business proposal ! Why work for somebody else when you can become rich in 18 WEEKS ! Have you ever noticed nobody is getting any younger plus more people than ever are surfing the web ! Well, now is your chance to capitalize on this . We will help you deliver goods right to the customer's doorstep and decrease perceived waiting time by 170% ! You can begin at absolutely no cost to you ! But don't believe us ! Prof Jones of Vermont tried us and says "My only problem now is where to park all my cars" ! We are a BBB member in good standing . DO NOT DELAY - order today ! Sign up a friend and you'll get a discount of 50% ! Thanks!

As you can see, the message has the look and feel of actual Spam. You can see how easily it would be to pass secret messages virtually undetectable between email accounts. This concept is what's really important. What I've shown is how you can use a third party application to encode and decode messages to mimic Spam. If you read the mail message, it does have issues with clarity and actually looks to have multiple messages run together which is odd. The idea here is to fool the user into thinking it's a useless message and it gets deleted without more than a couple of sentences being read. The important thing here is the concept itself. How often have you just deleted this type of message without really reading it? The same could be true for law enforcement officials actively looking for communications between suspected parties. Maybe this message gets overlooked because it looks like harmless junk email. That is exactly the point.

MP3Stego

MP3Stego is a steganographic tool used to hide data in MP3 files. Because of near CD quality and great compression ratios of about 11 to 1, MP3 files have gained worldwide use and offer a very good medium for information hiding. MP3Stego hides data during the compression process. It first compresses the data, encrypts it, and then injects it into the bit stream. This injection takes place at the inner_loop portion of the MPEG audio Layer III encoding process. The inner_loop quantizes the input data and increases the step size until the data can be coded with the available number of bits.[5]

OutGuess

OutGuess is a steganographic tool used to insert hidden information into the redundant bits of data sources. The basis of the program is the extraction of redundant bits for use in embedding and write them back after modification. The thing that makes OutGuess unique is the ability to preserve frequency counts statistics, which is a main property used in detection of steganographic content. OutGuess automatically determines the maximum message size that can be hidden in an image and still be able to maintain frequency count statistics to avoid detection.[6]

JPHS (JPHide and JPSeek)

JPHIDE and JPSEEK are freeware programs that allow you to hide data within a JPEG file. The Author of the programs designed them in such a way so as to make it nearly impossible to prove that the image contains hidden data. By keeping an insertion rate of 5% or less, the author believes that its impossible to conclude that there is any hidden data without having the original image to compare against. The basic rule of steganography is that as the insertion percentage increases the statistical nature of the jpeg coefficients differ from normal. Typically an insertion rate of greater than 15% starts to affect the image enough to become visible to the naked eye. The author suggests using host images that have a lot of fine detail, as they are better at hiding the effects of the data hiding.[7]

Detection

Two men by the names of Niels Provos and Peter Honeyman from The Center for Information Technology Integration at the University of Michigan set out to discover if such hidden communication was actually happening, and also develop the framework in which to detect it. The paper developed describes a stenography detection initiative using a web crawler to download JPEG images from the Internet. Then using the statistical analysis results of the images obtained from Internet, a set of images likely containing steganographic material would be generated. Once the set of images is compiled, further analysis of the images would be needed to actually obtain the hidden data hidden within.

[5] http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/
[6] http://www.outguess.org/
[7] http://linux01.gwdg.de/~alatham/stego.html

The team decided on searching for images that would have been impregnated with steganographic data using Jsteg/Jsteg-Shell, JPHide, and Outguess. All three of these steganographic tools are available freely on the Internet. To analyze the images for the statistical possibility of hidden data and also to reveal that data Stegdetect and Stegbreak were used. They are also freely available on the Internet. The framework of the detection system would follow a basic pattern; first the crawler would pull JPEG images from the internet, the analysis tool Stegdetect would analyze each image for the possibility of steganographic data, then using Stegbreak, the images in question were checked for hidden content.[8]

Provos and Honeyman turned to the auction site eBay to conduct their evaluation. At the time of the writing of the report (August 31, 2001), the web crawler had downloaded over 2 million images. Stegdetect determined 17,000 of these images possibly had steganographic content. Of those 17,000 images, stegbreak had been unable to verify the existence of any hidden data. It wasn't until October 12, 2001 that the first steganographic image was found in the wild. "In the wild" refers to the image being available on the Internet for anyone to download. ABC had covered a story about steganography. In the story an image called sovereigntime.jpg was shown and was supposed to contain a hidden image of a B-52 bomber, suggesting terrorist usage of steganography. Using their detection framework, the image was analyzed and the steganographic data was extracted. It contained a harmless picture of the B-52 graveyard at the Davis-Monthan Air Force Base. The image turned out to only be a demonstration.[9]

Conclusion:

By the amount of free and commercial tools available today, one can deduce that the use of steganography is growing. Even though the work of Provos and Honeyman revealed only one image out of over 2 million that they have run detection tools against actually contained a hidden message, the point is that it can happen, and still may be happening considering the amount of different tools that weren't accounted for in their research. Awareness of the use of steganography is the first step. Steganography is just another tool for someone to use to hide data, and I believe will be used more often in the future, whether for covert communication or personal data concealment. Security professionals will surely need to be aware of its existence as its use becomes more prevalent.

[8] Niels Provos, Peter Honeyman,Detecting Steganographic Content on the Internet, Section 1, http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

[9] http://www.citi.umich.edu/u/provos/stego/abc.html

[1] Niels Provos, Peter Honeyman,Detecting Steganographic Content on the Internet, Section 1, http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

[2]Dr Anthony Ho, Internet Business 99, Singapore, 24th June 1998, Page 2, http://www.datamark-tech.com/publications/steganography.pdf

[3] Niel F. Johnson, Steganography, http://www.jtc.com/stegdoc/stegdoc.html, Section 2.2

[4] http://www.spammimic.com/

[5] http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/

[6] http://www.outguess.org/

[7] http://linux01.gwdg.de/~alatham/stego.html

[8] Niels Provos, Peter Honeyman, Detecting Steganographic Content on the Internet, Section 1, http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

[9] http://www.citi.umich.edu/u/provos/stego/abc.html