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 (Security 401)"
at http://www.giac.org/registration/gsec

Hiding in Plain View: Could Steganography be a Terrorist Tool?

Tom Kellen – GSEC Practical Assignment v1.2f

The events of September 11, 2001 catapulted awareness of terrorism to the forefront of every mind in every civilized culture in the world. They have also raised interest in the ways that terrorists may have communicated and planed these events. Earlier this year, in a USA Today article it was suggested that terror groups may be using the Internet to pass information using techniques including e-mail, chat rooms, bulletin boards and other web sites[1]. There is also much speculation that these groups may be using technologies like encryption and steganography to help hid their communications.

Many people have heard of cryptography or encryption since those are techniques that are commonly used in business today. Steganography, however, is a technology that may not be as familiar. The word steganography comes from the Greek *steganos* (covered or secret) and – *graphy* (writing or drawing) and literally means, covered writing.[2]

Steganography has been around for hundreds of years and its main purpose is to pass information in a way that the leaves the casual observer unaware. One of the first recorded uses of steganography was related by the Greek historian Herodotus. He tells of how one of his countrymen sent secret messages by writing them on the wooden base of wax tablets[3]. The wax on top was blank; therefore the tablet was thought not to contain any information. The most familiar form of steganography would be that of using invisible ink to write a message. During World War II, this method, among many others, was used by the Allied and Axis powers. These messages were often written using fruit juice, milk, or urine which would darken to reveal the message when heated. The practice of using small punctures above key words to reveal a hidden message within another message was also frequently used.

Cryptography and steganography are often lumped together even though they are very unalike, yet complementary, technologies with different purposes. Cryptography attempts to change the contents of a file or message in such a way that it is not readable by someone who is not the intended recipient. The intended recipient would have a key that would allow the encrypted file to be unlocked and viewed as planned by the sender. One problem with encryption is that it does nothing to hide the fact that a message is being transferred and in fact may even make it more obvious. Its strength is in the difficulty of figuring out the means of encryption and the key to decrypt the message.

Steganography, on the other hand, attempts to hide the message in such a way that the observer may not even realize that the message is being exchanged. Combining the two technologies provides a method of communication that is not only difficult to find but also to decipher. The ability to make intercepting stego-files difficult and to disseminate them so easy has lead to the rise in their use by not only privacy fanatics

© SANS Institute 2000 - 2005 Author retains full rights.

but also possibly by the terrorist community[4].

In the digital age, steganography can take many different forms; the most common structure is hiding one file within another file. This is typically done using image, audio or video files that are commonly found on the Internet. Stego tools do this in such a way that the human eye or ear is unable to tell the difference in the changed file. A quick search of the Internet reveals programs to allow for hiding files within BMP, JPG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MP3, AVI, TIF, TGA, DLL and EXE files. Many of these programs can also encrypt the contents before hiding them in the carrier file.

According to the Washington Post, federal agents have found at least three years of evidence, "that bin Laden's group embedded secret missives in mundane e-mails and Web sites."[5] There is still no direct evidence that terrorists used these technologies in planning the Sept. 11th attacks, but it is certainly not beyond the realm of imagination. In fact, in a briefing given in late September by the FBI, the FBI's Assistant Director Ron Dick, head of the National Infrastructure Protection Centre stated that "the hijackers had used the net, and 'used it well'."[6] Since there is no direct evidence as to how the terrorists communicated to coordinate this attack, let's investigate some of the possibilities that they could have used.

Using image files to transfer information is the method that first comes to mind. Many newspapers have reported that "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."[7] This may sound difficult to do on the surface but in actuality is a simple and effective way to pass information.

Nearly every site visited on the Web contains graphics of some sort. Most probably don't register except peripherally on the browser, but they could be the perfect place to put carrier stego-files. It has been suggested that these terrorist groups posted carrier files on porno sites which may seem an ironic place for Muslim fundamentalists to place their files, but this would also go along with the premise of hiding in plain view.

The pictures on pornographic sites are typically large in size and use a large amount of colors. These would make ideal carrier files. The larger the original file, the larger the payload it can carry. Stego tools that work on graphic files typically embed the payload file by changing the least significant bit (LSB) in each pixel of the file. These programs use these LSB's to hold the data for the payload file. Larger carrier files would have more pixels and could therefore carry more information.

The difficulty with many porno sites is that they are "pay for use" and would require someone on the inside to post the files to the site. While this could easily be done, another possibility is using more publicly available sites. There are many Internet news groups that are used for passing and posting of graphic images that could also serve as ideal places to post this type of information.

© SANS Institute 2000 - 2005 Author retains full rights.

Another possible scenario is that public auction sites like eBay and Amazon might be good places to post these files. Imagine that instead of a porno file, a person takes a picture of something they are supposedly selling, say an automobile. He then runs the picture through a stego tool and then posts it to eBay as part of an auction. Millions of people may look at that picture never knowing that it contains plans for a terrorist attack. Only the intended recipient who knows what to look for and downloads the file will receive the real message by running it back through the same stego tool.

The vast size of the Internet is also a great boon for those trying to hide information. Posting information to public sites is not the only way to make them available for the intended recipient. It seems like most everyone who has a connection to the Internet, has some sort of home page posted. Even those without permanent connections can get a free web site at places like Geocities or Tripod. How difficult would it be for a terrorist to put up one of these small free sites and make it appear to be an innocuous tribute to their pet cat? The chances of ever stumbling across the site are remote and it would probably never be seen except for those who knew where to look.

Terrorists could also have cell members working in major corporations, or at Web hosting providers, that have access to those company's web sites. It is not inconceivable that a graphic image on a company's web site could contain terrorist information totally without that company's knowledge.

Some of these postings may not even be covert. Eric Cole, noted security expert, author and lecturer, told one class at the Oct. 2001 SANS conference that he had been involved in a project that monitored a known terrorist sympathizer Web site. Eric wrote a program that downloaded an image on the main page every 10 minutes and after analysis it was found that while visually the image did not appear to change, statistically it changed every hour. It is reasonable to assume that there may have been a payload carried in that image and that it was changed constantly to either share more information or to make it harder for security agencies to find out the information contained within the picture.

According to Neil Livingstone, a terrorism expert at Global Options LLC in Washington, DC, the U.S. government monitors more than 5,000 Web sites devoted to terrorism and criminal activities. With an estimated 28 billion images and over 2 billion Web sites on the Internet, it is an impossible task to find these stego-carrier image files.[1] The possibilities are endless for hiding information within images on the Internet.

Image files are not the only medium that steganography techniques could use to transfer information. Audio files like WAV, MID, AU, and MP3 are also ideal carriers and are nearly as ubiquitous on the Web as are image files. There are almost as many steganography tools for audio files as there are for image files and they are just as easy to use.

Some articles have reported that terrorists like Osama bin Laden have hired computer

© SANS Institute 2000 - 2005 Author retains full rights.

experts to assist with this type of information hiding. It does not take a computer expert to use these freely available tools. It would be very easy for even a computer neophyte to hide and post information.

An example of the simplicity to conceal information is the program MP3Stego. This free program "will hide information in MP3 files during the compression process."[8] The program first encrypts the data, then compresses it, and finally hides the data within the MP3 bit stream. With a command as simple as:
encode –E hidden_text.txt –P pass svega.wav svega_stego.mp3
the operator will have an MP3 file with a hidden and encrypted message within. On the other end, the operator gives the command:
decode –X –P pass svega_stego.mp3
and the hidden message is uncompressed, decrypted and placed into the file svega_stego.mp3.txt. As long as both parties know the password, it does not take a computer expert to prepare or use these types of files.

One way to try to determine if stego-files are being used to pass information would be to watch peoples browsing habits on web sites. With image files, it is easy to watch for users who visit a web site to just download particular images and do not browse the rest of the site. They may be harvesting stego-files. On the other hand, audio files can be embedded into the HTML of web pages so that they automatically play when someone visits the Web page. What actually happens is that these files are downloaded into the visitor's "temporary internet files" directory and played from there. It would be impossible to determine if the visitor is deliberately looking for such a file or not. The terrorist would only have to retrieve the audio file from their "temporary internet files" directory at a later time and decode it at their leisure.

Audio files have also become very popular on Peer-to-Peer sharing networks such as Napster and Gnutella. These networks could be ideal ways to transfer these files; the terrorist would just use the pre-built network and would only need to know the correct location to download the file from.

Another benefit of the audio format of carrier files is that it can easily be hand carried to make finding its transmission even more difficult. Data could easily be hidden in MP3 files and then transferred to an MP3 player and carried by a terrorist to various locations. These MP3 devices have become so popular that if someone were stopped and such a player were found in their possession, it would raise no suspicion and would probably not be investigated further. The same holds true for WAV files. These could be burned onto a CD and a music CD would raise much less suspicion that would a CD filled with images. According to MSNBC, "Bin Laden relies on human messengers, safe houses and close-knit groups such as family members to send out his directives."[9] It is not hard to imagine maps and plans being transferred using the latter mentioned methods.

At 9 a.m. on Sept. 11, the U.S. secret service received a message that read, "Air Force One is next."[10] What was so scary about this message was that it was transmitted

© SANS Institute 2000 - 2005 Author retains full rights.

using the White House's top-secret code words for that day. It seems obvious that the terrorists must have someone on the inside at the highest levels of U.S. government. But how could such a mole get such sensitive information out of supposedly secure installations? Steganographic techniques would certainly be one possibility.

During the Cold War one favorite technique for passing covert information was the use of a "dead drop." Using this method one party would make a chalk mark on a mail box indicating that a package was waiting in a pre-arranged location and the other party upon seeing the mark would know to go pick up the package. In this way, the two parties would never have to meet or even know who each other are. This is ideal because if one party is captured they have no information that might implicate the other person. In a sense, the whole Internet can now be considered a huge "dead drop" using stego-carrier files. Using these techniques makes it difficult to determine who the two parties in communication are. This is why using steganographic techniques may be becoming more popular than e-mail which can be traced from sender to receiver.

While using steganography may seem an ideal way for terrorists to hide information, it is far from perfect. According to many researchers the current generation of stego programs doesn't really work well.[3] Most of the programs leave some sort of fingerprint behind that allows careful observers to know that something is going on. The easiest way to determine whether a file has a stego payload is to be able to compare it to an original. This is probably much easier with audio files where there may be many copies of the same file without a payload for comparison. Image files often prove much more difficult as access to the original is often not possible.

Another problem with locating stego files is the size of they payload file. The smaller the payload file, the harder it is to find. For instance, a one bit, "yes" or "no" message embedded in an MP3 file would be nearly impossible to find.

One company, WetStone Technologies, Inc., has recently released their Stego Watch service. Their Steganography Director examines images, and based on a mathematical model tries to determine if steganography is used or if the image is pristine. While this may be a first step in a war against these techniques, it really only works for legitimate organizations to maintain their integrity by routinely having their networks scanned.[11] This might close one avenue of communication, but the real problem is the sheer volume of information and files available on the Internet.

Although steganography programs hold the possibility of being terrorist tools, all of the evidence of terrorist's use of these tools has, so far, been inferential. While the FBI has found that three of the suspected hijackers rented a room in Hollywood, Florida and demanded 24-hour internet access, they have no way of knowing exactly what they were doing on the Internet.[12]

The FBI says that in the evidence they have found so far the terrorists did not use concealment or even encryption techniques. E-mails they have found were easily read

© SANS Institute 2000 - 2005 Author retains full rights.

and the only stealth was the use of code words such as referring to bin Laden as the "director" instead of calling him by name. A team of researchers from the University of Michigan reported a few days before the attacks that they had used a network of computers to search for the "signature" of steganography. "According to researchers at the Centre for Information Technology Integration, they 'analyzed two million images but have not been able to find a single hidden message'."[6]

Can steganography be used as a terrorist tool? The answer is an unequivocal yes. The possibility for the abuse of steganography techniques by terrorists is obvious. The mind just needs to ponder for a short time to imagine a multitude of ways to exploit this technology. Several examples of abuse have been cited in this paper. Whether these techniques have been used yet is still open to debate, but the opportunity for terrorists to add steganography to their tool kit is undeniably at hand.

Awareness is going to be one of the greatest weapons in this War against terrorism. Hopefully this paper will raise some consciousness about tools that could be used by terrorists to further their goals. Just as encryption is not "bad" in and of itself, steganography is not "bad"; it is just another tool which can be used by bad people for evil purposes. Technology and the Internet will obviously play an important role in the War and will work equally well for both sides. Vigilance and perseverance will be the only way to overcome terrorist and win the War against terrorism.

---

[1] Kelley, Jack. "Terror groups hide behind Web encryption." USA Today. 19 June 2001. URL: http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm (6 Nov 2001)
[2] "Steganography (Hidden Writing). URL: http://www.wepin.com/pgp/stego.html (7 Nov 2001)
[3] McCullagh, Declan. "Secret Messages Come in .Wavs". Wired News. 20 Feb 2001. URL: http://www.wired.com/news/print/0,1294,41861,00.html (6 Nov 2001)
[4] Auer, Catherine. "Behind the bits". Bulletin of the Atomic Scientists. May/June 2001. URL: http://www.bullatomsci.org/issues/2001/mj01/mj01auer.html. (6 Nov 2001)
[5] Cha, Ariana Enjung and Krim, Jonathan. "Terrorists' Online Methods Elusive". 19 Sep 2001 URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A52687-2001Sep18
[6] Campbell, Duncan. "How the terror trail went unseen". 10 Aug 2001. URL: http://www.heise.de/tp/english/inhalt/te/9751/1.html (6 Nov 2001)
[7] Schneier, Bruce. "Terrorists hide messages in messages". MSNBC. 25 Sep 2001. URL: http://stacks.msnbc.com/news/633709.asp
[8] Petitcolas, Fabien A. P. "MP3Stego". 10 Aug 2001. URL http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego
[9] Associated Press. "Bin Laden foils U.S. technology". MSNBC. 20 Sep 2001. URL: http://stacks.msnbc.com/news/631609.asp (6 Nov 2001)
[10] "Digital moles in the White House?". WorldNetDaily. 20 Sep 2001. URL: http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=24594
[11] Gordon, Dr. Gary. 'WetStone Announces Stego Watch[tm] Service". WetStone Technologies, Inc. 4 Oct 2001. URL: http://www.wetstonetech.com/pr0184.htm (6 Nov 2001)
[12] "France terror code 'breakthrough'". BBC News. 5 Oct 2001. URL: http://news.bbc.co.uk/hi/english/world/europe/newsid_1580000/1580593.stm (6 Nov 2001)

© SANS Institute 2000 - 2005 Author retains full rights.