DIGITAL FORENSICS
/ MAGAZINE
Issue 03 1 May 2010

DIGITAL STEGANOGRAPHY

AN INTRODUCTION TO THE PRACTICE OF DIGITAL INFORMATION HIDING

Learn why digital steganography is one of the biggest threats to forensics investigations and why it's only a matter of time...

by James E. Wingate

/ ENTRY

Throughout history man has sought ways to communicate secretly. One of the earliest recorded methods for doing this was the use of wax tablets by the ancient Greeks.

In 480BC, Demaratus used wax tablets in an attempt to warn King Leonidas of Sparta that King Xerxes I planned to lead his army into Greece prior to the historic Battle of Thermopylae. Because the danger of being discovered was great, Demaratus hid his warning by scraping the wax off the tablets and scribing his message directly onto the wood. Then he recoated the tablets with wax and sent the tablets via messenger to Leonidas. Interestingly, when the tablets were delivered, no one could figure out why they had received wax tablets with nothing written on them. According to The Histories written by Herodotus, widely acclaimed as the Father of History, Queen Gorgo, Leonidas' wife is purported to have said, "If they would scrape the wax off the tablet, they would be sure to find the writing upon the wood." Thus, the warning was delivered, but the Spartans got massacred at Thermopylae in one of history's greatest last stands as depicted in the movie "300" starring Gerard Butler.

Demaratus' use of wax tablets is one of the earliest and most widely referenced uses of information hiding, a practice that has become known as steganography.

/ WHAT IS STEGANOGRAPHY?

Steganography is derived from the Greek words "steganos", which means, "covered" or "protected" and "graphein" which means "writing." When the two words are combined, the result is literally "covered writing" or "protected writing."

Essentially, steganography is a means of communicating secretly, or covertly. Over the years the art of Information Hiding has presented itself in many ways, for example:

- The Chinese hid secret messages on slips of paper and baked them in moon cakes
- Mary, Queen of Scots, hid encrypted information in the bunghole of beer barrels
- Gaspar Schott hid information in musical symbols used to write sheet music
- George Washington used invisible ink to communicate secretly
- Microdots, the size of a period, were used in World War II to conceal information[1]

For a comprehensive history of secret communication from Ancient Times to the present, the interested reader should read The Code Breakers by David Kahn[2].

In the Internet era, steganography has evolved from to a digital form of information hiding. Accordingly, when talking or

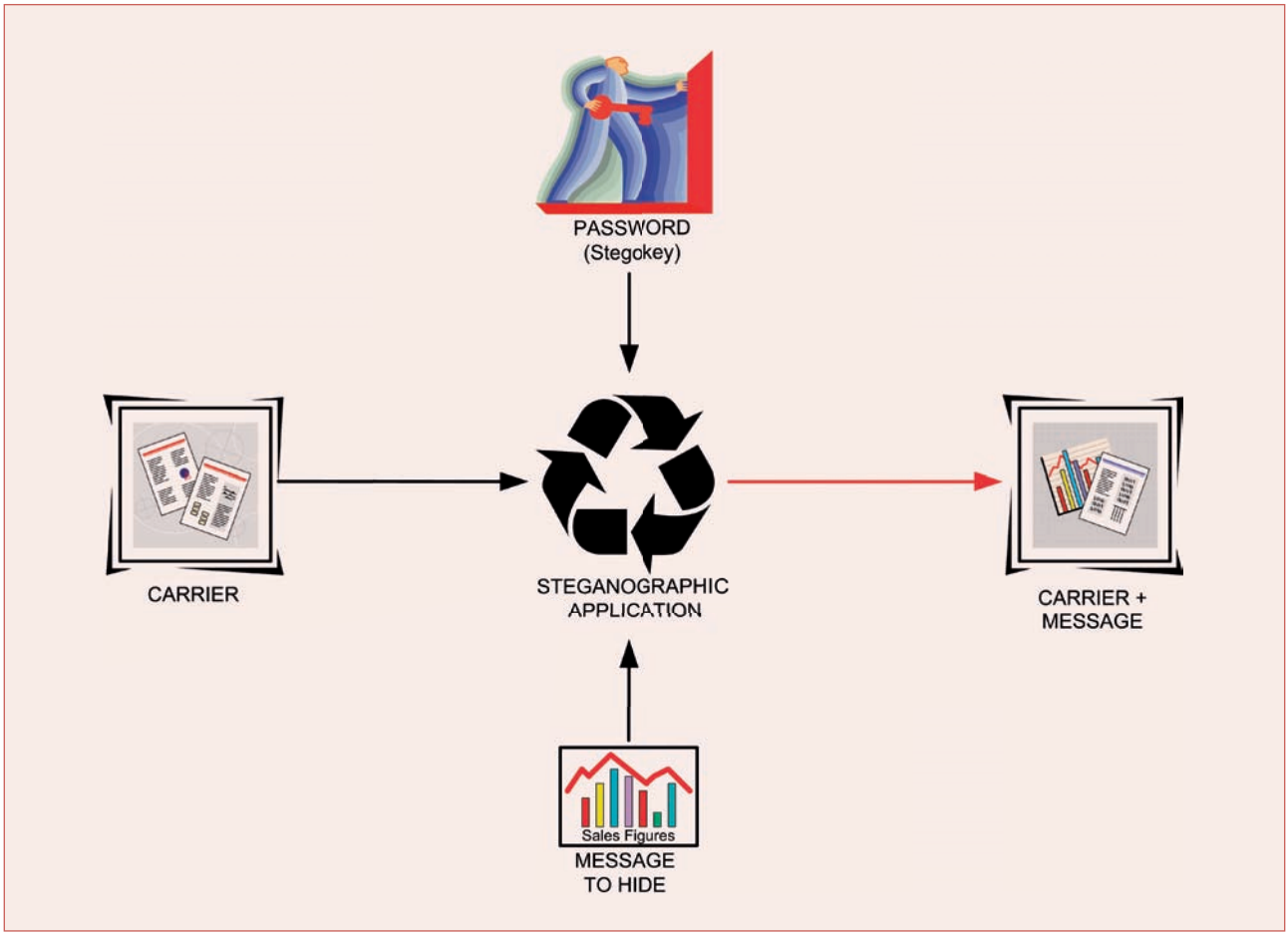


Figure 1 . Basic Steganography Model

DIGITAL STEGANOGRAPHY IS ESSENTIALLY ABOUT HIDING A FILE IN, OR APPENDING A FILE TO, ANOTHER FILE, CALLED THE CARRIER FILE

writing about steganography today, it is generally presumed the speaker or writer is referring to digital steganography.

Digital steganography is essentially about hiding a file in, or appending a file to, another file, called the carrier file, such that the carrier file is not altered enough to raise suspicion that something may be hidden within it or appended to it. A basic Steganography model can be seen at Figure 1.

There are a number of techniques used for information hiding for example a technique called spam mimicry where information is hidden by disguising it as spam (www.spammimic.com) or disguising the information as a nonsensical but often humorous one-act play as does Sam's Big Playmaker.

A technique exists where hiding information in the unused fields of communication protocols such as IPv4 and IPv6. Using a tool called voodoon3t (VooDooNet) you can hide information in unused IPv6 fields encapsulated in IPv4 packets, this was introduced at DEFCON in 2006. The tool effectively creates a tunnel for funnelling hidden information through current generation network security appliances because most have yet to be programmed to inspect IPv6 packets.

Another very new technique emerging is the ability to hide information in digitized voice streams generated by the growing number of Voice over Internet Protocol (VoIP) systems being deployed. Modifying the low order bits of digitized voice signals ever so slightly hides information in a way that the hidden information does not affect the quality of the digitized voice signal.

/ WHY USE STEGANOGRAPHY?

A frequently asked question is "Why would anyone want to go to the trouble of using steganography to hide information when they can use cryptography to encrypt it?" The primary reason is because cryptography is an overt form of information hiding, or information protection. The fact that information has been encrypted is easily detected which can lead to attempts to decrypt the information, some of which might be successful.

However, the main reason steganography is appealing is because it is a covert form of information hiding, or information protection, that conceals the very fact the information even exists! As an added measure of security, information can be encrypted before being hidden as

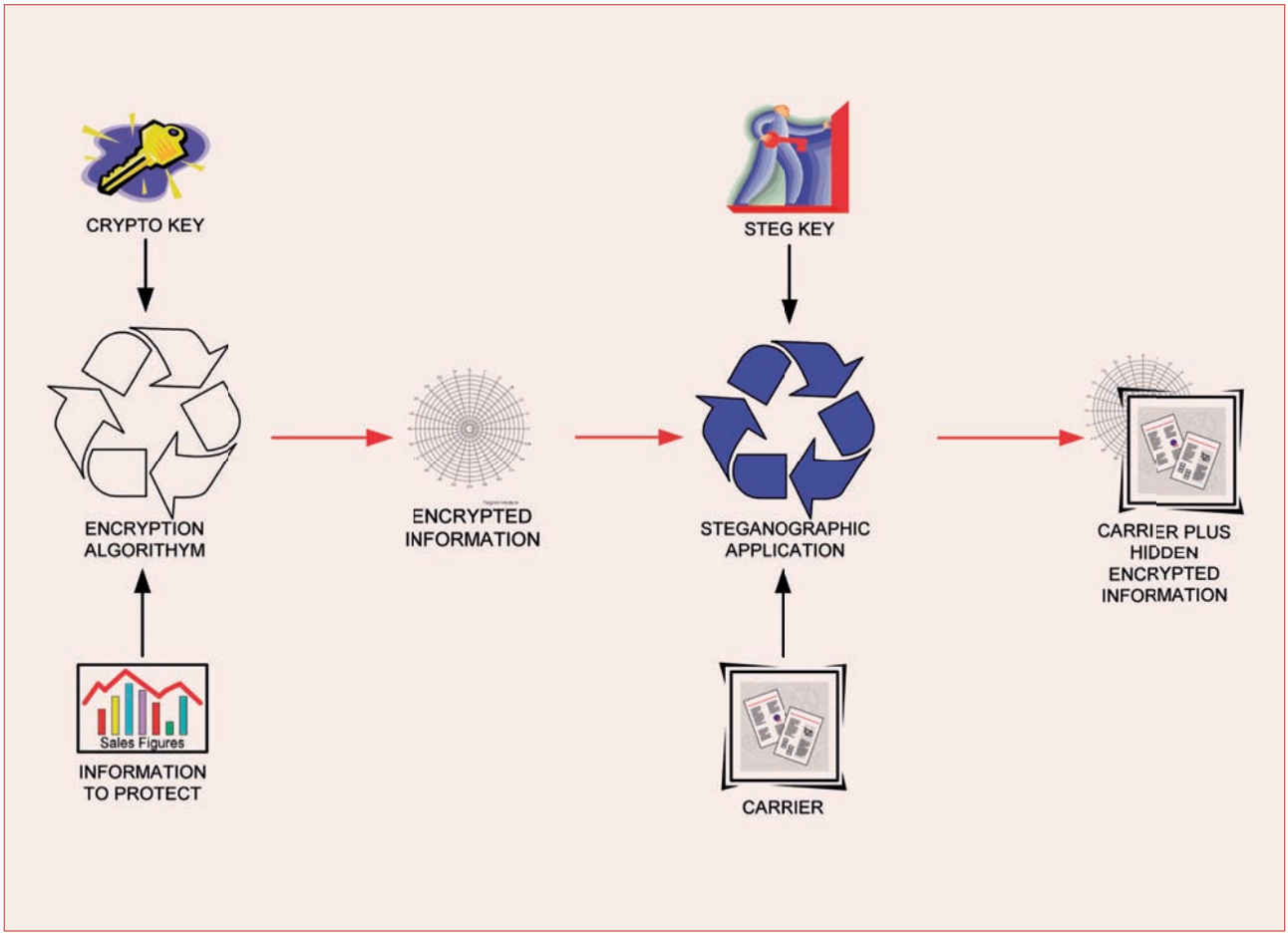


Figure 2. Advanced Steganography Model

illustrated in Figure 2. For this reason, steganography is often referred to as the Dark Cousin of cryptography.

Another reason to use steganography is simply because it is so readily available. It is estimated that there are well over 1,000 digital steganography applications available on web sites across the Internet. Most of the applications are available as freeware or shareware.

While the word steganography might not pop into the head of the average user, the words "information hiding" probably would. Entering those words in a Google search yields over eight million links, many of which lead the user to web sites containing steganographic applications. For example, the interested reader can visit www.stegoarchive.com where over 100 steganographic applications can be found.

These applications are not only easy to find, they are easy to download, install, and use. It does not take an expert computer user to use the applications because they come equipped with the familiar drag-and-drop or wizard interface that the majority of users have learned to use as a basic computer skill.

/ WHO USES STEGANOGRAPHY?

Insiders, paedophiles, drug traffickers and terrorists, to name a few. Anyone who wants to cover their digital tracks could use steganography as a counter forensic investigation technique. Human Nature 101 taught us that people doing bad things and fear getting caught and doing time in the 'Cross-Bar' hotel will attempt to hide what they are doing.

IT IS ESTIMATED THAT THERE ARE WELL OVER 1,000 DIGITAL STEGANOGRAPHY APPLICATIONS AVAILABLE ON WEB SITES ACROSS THE INTERNET

Insiders with access to sensitive information such as protected health information, or PHI, and personally identifiable information, or PII, or large quantities of intellectual property can use steganography to exfiltrate (i.e., steal) information. These days, most insiders have access to large quantities of sensitive information. They can easily steal the information by hiding it inside seemingly innocuous looking images and then upload the images to a web site or send the images to themselves, or a co-conspirator, as an email attachment. Who would suspect pictures of a vacation to the beach, mountains, etc. would contain hidden information? No one would.

A common means of distributing child pornography is to use steganography to embed the images inside of other images and then upload the images to a web site.

For example, who would suspect that pictures of a train collection for sale on eBay would contain child pornography? No one would.

Narcotics traffickers can use steganography to conceal information about their drug deals. In a case from the not too distant past, the notorious Colombian drug trafficker, Juan Carlos Ramirez Abadia, was arrested in Brazil. It had been discovered he was using pictures of Hello Kitty to send messages to his minions about cocaine shipments between countries.

Finally, there are the terrorists. Steganography is a perfect tool for members of terrorist cells to communicate covertly and is being used on several Jihadist web sites. In fact, the February, 2007 edition of Technical Mujahid, a training manual for Jihadis, contains an article that encourages extremists to download a copy of the software program Secrets of the Mujahideen. As previously mentioned, steganography is being increasingly used as an anti-forensics tool to make it even more difficult, and in most cases impossible, for law enforcement digital forensics examiners to recover digital evidence.

STEGANOGRAPHY IS A PERFECT TOOL FOR MEMBERS OF TERRORIST CELLS TO COMMUNICATE COVERTLY

/ HOW MANY ARE USING STEGANOGRAPHY?

No one really knows. Obviously, everyone isn't using it but it is equally obvious that some are using it. The answer lies somewhere in between no one and everyone.

Steganography presents an interesting paradox. It is difficult to convince people to be concerned about something they cannot see. However, electricity is a glaring exception to that; we can't see it but we sure know it's there and have learned to treat it with proper respect or risk injury or even death.

Because there is no large body of empirical evidence that steganography is being used, most digital forensic examiners and network security managers don't believe it is being used. Accordingly, they are not sufficiently concerned enough to acquire and employ tools to detect its use.

It must be noted, however, that if only one insider used steganography, they might use it to steal the crown jewels. It is conceivable that this could cause a company to go out of business. Thus, while the risk may be perceived to be low to non-existent, the impact can be disastrous; even fatal.

/ FUTURE OF STEGANOGRAPHY

Certainly, as the capabilities of network security tools, such as Data Loss Prevention systems, continues to improve, the appeal of using steganography to steal sensitive information will continue to grow. We have reached a point where information is more valuable than money or at least as valuable as money. The issue with money is that once spent, it is gone. However, information can be sold, and resold, many times on the burgeoning black market for practically any kind of information anyone wants to sell.

It would be instructive to remember Willie Sutton's philosophy about banks. Willie was a prolific bank robber who stole more than two million dollars from over 100 banks between the late 1920s until his final arrest in 1952. When asked why he robbed banks, Willie reportedly said "Because that's where the money is."

So today we could ask cyber criminals a similar question. Why do they rob networks. The answer would surely be "Because that's where the information is."

Use of steganography to steal information or otherwise conceal evidence of criminal activity will continue to grow. However, it will not be detected until more examiners and security managers' start looking for it.

To state the obvious, "that which is not looked for will never be found". /

/ MORE INFO

Information Hiding – Techniques for Steganography & Digital Watermarking – Katzenbeisser, Petitcolas, © 2000 Archtec House Inc, ISBN 1-58053-035-4

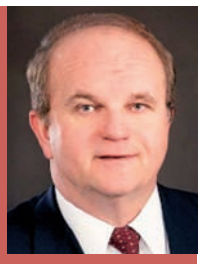
Information Hiding – Steganography & Watermarking Attacks & Countermeasures – Johnson, Duric & Jajodia, © 2001 Kluwer Academic Publishers, ISBN 0-7923-7204-2

Steganography in Digital Media: Principles, Algorithms & Applications – Jessica Fridrich, © 2009 Cambridge University Press ISBN-13 978-0521190190

REFERENCES

1. Gregory Kipper, Investigator's Guide to Steganography, Auerbach Publications, October 2003, ISBN 978-0-8493-2433-8
2. David Kahn, Simon & Schuster; 2nd Revised Edition (6th Oct 1997) ISBN 978-0684831305
3. Sams Big Playmaker, HYPERLINK "http://www.scramdisk.clara.net/play/playmaker.html" www.scramdisk.clara.net/play/playmaker.html, Last Modified 10 Feb 2000. Copyright SecurStar GmbH, 2000

/ AUTHOR BIO



James E. Wingate, CISSP-ISSEP, CISM, CHP, CHSS, is Director of the Steganography Analysis and Research Center (SARC) and Vice President of Backbone Security. He is leading efforts to develop state-of-the-art digital steganalysis tools for use by digital forensics examiners and network security personnel in the public and private sectors. He is a member of HTCC and HTCIA and regularly gives presentations on the use of digital steganography to conceal evidence of criminal activity at major conferences across the United States. He retired from the US Air Force after more than 24 years of service as a Communications and Information officer. He holds a B.S. in Computer Science from Louisiana Tech University, Ruston, Louisiana, and an M.S. in Computer Engineering from the University of South Florida, Tampa, Florida.

Contact information:
Email: jwingate@backbonesecurity.com
Office: 304.366.9161
Toll Free: 877.560.SARC