Covert Computer and Network Communications

Robert C. Newman, CISSP
Lecturer of Information Systems
Georgia Southern University, Statesboro, Ga. 30460
912-486-7563
newmanrc@georgiasouthern.edu

ABSTRACT
The ex-filtration of confidential information across communication networks is a challenging problem. It is possible for transmissions to be hidden or masked in such a way to circumvent the security policies of an organization. An objective might be to make contacts “invisible” to all parties except designates. This can take the form of a covert channel [3]. A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy."

Covert channels can be the vehicle used to breach a computer network for the purpose of downloading tools from outside, uploading internal data to the outside, and communicating to outside parties. Internal users may want to use forbidden protocols, have non-malicious backdoor access, and hide their actions from management. Covert channels provide an alternative, subversive means of achieving confidentiality and maintaining anonymity.

Categories and Subject Descriptors
K.4.1 [Computers and Society]: Public Policy Issues * ethics, human safety, privacy.

General Terms
Covert channels, covert storage channels, steganography, security

Keywords:
Covert channels, steganography, security

1. INTRODUCTION
An important issue within organizations today is the possibility of confidential information leakage. Detection of information leaks is a challenging problem as most organizations utilize a broad and diverse communications network. It is difficult to determine which communication traffic is legitimate and that which consists of malicious data ex-filtrations.

Information Security Curriculum Development Conference’07,
September 28-29, 2007, Kennesaw, Georgia, USA.

Confidentiality of communication transmissions can be achieved by cryptography, via encryption, or covert methods, such as steganography. In some cases, message content is not as important as the identities of the parties communicating. Encrypted communications, which can be detected, might cause additional interest in determining message content. An objective might be to make contacts “invisible” to all parties except designates.

A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy" [9]. Essentially, it is a method of communication that is not part of an actual computer system design, but can be used to transfer information to users or system processes that normally would not be allowed access to the information.

A covert channel is so called because it is hidden within the medium of a legitimate communications channel. Covert channels typically manipulate certain properties of the communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information through the medium without detection by anyone other than the entities operating the covert channel.

Covert channels can be the vehicle used by crackers who have breached a computer network. This breach could allow for downloading tools from outside, uploading internal data to the outside, and communicating to outside parties. They can also be used by internal users who want to use forbidden protocols, have non-malicious backdoor access, and want to hide their actions from management. Covert channels provide an alternative, subversive means of achieving confidentiality and maintaining anonymity [4].

2. COVERT CHANNELS DEFINED
The **Trusted Computer Security Evaluation Criteria (TCSEC)** is a set of criteria established by the National Computer Security Center, an agency managed by the United States' National Security Agency [1]. These standards have now been superseded by the **Common Criteria**. The term covert channel is defined in the TCSEC specifically to refer to ways of transferring information from a higher security classification compartment to a lower classification.

The TCSEC defines two kinds of covert channels:

2.1 Storage channels - Communicate by modifying a stored object. This covert channel involves the direct or indirect writing to a storage location by one process and the direct or

indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (*e.g.*, sectors on a disk) that is shared by two subjects at different security levels [1]. Examples of such channels include hiding data in unused fields of RFC-defined protocols like Internet Protocol (IP), Transmission Control Protocol (TCP), ICMP, and HTTP.

2.2 Timing channels - Transmit information by affecting the relative timing of events. A covert channel process signals information to another process by modulating its own use of system resources (*e.g.*, CPU time) in such a way that this manipulation affects the real response time observed by the second process. The subject of covert timing channels is very complex in nature requiring computer scientist and computer engineering expertise [1]. The emphasis of this document will be oriented towards covert storage channels.

Covert communication channels, sometimes called subliminal channels, are often motivated as being solutions to the "prisoners' problem" [8]. Consider two prisoners in separate cells who want to exchange messages, but must do so through the warden, who demands full view of the messages (not encrypted). A covert channel enables the prisoners to exchange secret information through messages that appear to be innocuous. A covert channel requires prior agreement on the part of the prisoners. For example if an odd length word corresponds to "1" and an even length word corresponds to "0"; then the previous sentence contains the subliminal message "101011010011" (2771). In this problem the warden can monitor prisoner communications by reviewing all messages, and pass or deny them based on visual observations. The other option is to modify the messages slightly, not to change the meaning of the message itself, but ensure that it is not precisely the same as the original. This second option would destroy the content of any hidden message in the communication. Note the process is extremely time-consuming; however the prisoners have lots of time.

All covert channels draw their bandwidth (information-carrying capacity) from a legitimate channel; thus reducing the capacity of the latter; however, the bandwidth drawn from the channel is often unused, anyway, and so the covert channel may still be well hidden. Because any bandwidth used by the covert channel is "stolen" from the legitimate channel, the greater the bandwidth used by the covert channel, the more likely it is that it will be obvious to users of the legitimate channel.

A covert channel allows an attacker that has compromised a secure system component to leak sensitive information without establishing its own explicit connection to the outside world. Covert channels are notoriously hard to detect or eliminate, but this is somewhat ameliorated by the fact that their bandwidth is often rather low, and, in any case, exploiting them requires that the attacker somehow compromise a sensitive system component in the first place. The sensitive system component typically gives the attacker total control over the system or an output channel, making the threat of covert channels relatively minor compared with that of whatever software vulnerability which made such a compromise possible in the first place.

One of the primary techniques for implementing a covert storage channel is called steganography.

3. STEGANOGRAPHY (STEGO)

Steganography is the art of covered or hidden writing. The purpose of stego is covert communication to hide a message from a third party. Stego can be used to hide information in e-mail messages, on file transfer protocols (FTP) or Peer-to-Peer (P2P) sites, on auction, news, blog, or other sites. The stego process involves placing a hidden message within some transport medium, called the carrier or cover. In addition, the use of a stego key may be employed for encryption of the hidden message. Information can be hidden in images such Joint Photographic Experts Group (JPEG), Bitmap (BMP), Portable Network Graphics (PNG), Graphics Interchange Format (GIF), MS Word documents, text documents, MP3, EXE, DLL, and other formats. Stego techniques can also be employed in **digital watermarking**, which is a tool for protecting copyrights in a variety of digital audio, video, and software entities.

Steganography is also used to hide secret messages in other messages, such that the secrets' very existence is concealed. Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper. Historical tricks include invisible inks, tiny pin punctures on selected character, minute differences between handwritten characters, pencil marks on typewritten characters, grilles which cover most of the message except for a few characters, and so on.

Also associated with steganography is the field of **cryptology**, which encompasses both cryptography and cryptanalysis. **Cryptography** is the conversion of data into a secret code for protection of privacy using a specific algorithm and a secret key. The original text, or "plaintext", is converted into a coded equivalent called "cipher text" via an encryption algorithm. The cipher text can only be decoded (decrypted) using a predefined secret key. **Cryptanalysis** is the art and science of breaking and decoding cipher text, usually without prior knowledge of the secret key. Cryptanalysis reveals the secrets hidden by cryptography.

Steganography is a form of covert channel in which very small details of images are subtly altered in order to communicate information in a way not immediately obvious to anyone casually examining the images. The classification of stego techniques is depicted in Figure 1 [5, 7]. Linguistic steganography includes semagrams or open codes. Semagrams hide information by the use of symbols or signs. Open codes include jargon codes and covered ciphers. Jargon code uses language that is understood by a group of people, but is meaningless to others. Covered or concealment ciphers include both grille and null ciphers. The grille cipher uses a template to identify the message, whereas the null cipher hides the message according to some prearranged set of rules.

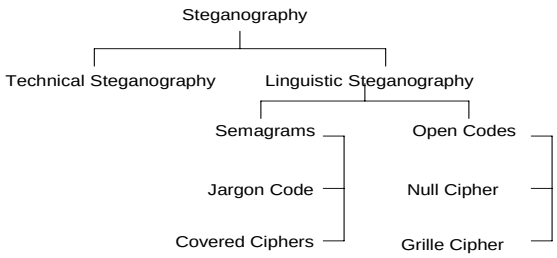


Figure 1. A Taxonomy of Steganography

3.1 Semagrams

Text semagrams work with graphical modifications of the text. They are tiny, however are still visible. Some examples include binary code, Morse code, tiny spaces, old typewriter effect, and real semagrams. Binary codes include the numbers 1 and 0 and are the easiest to implement using various techniques. Morse code is out-dated and not as flexible as binary codes. The 8-bit ASCII binary representation of the word "sex" is "010100110100010101011000 ", whereas the Morse code representation is "--- . -..- ". Binary is usually the code of choice in today's covert transmissions.

3.2 Null Cipher

A **null cipher** is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. It would today be regarded as a simple form of steganography. Null ciphers can also be used to hide ciphertext, as part of a more complex system. In classical cryptography a *null* is intended to confuse the cryptanalyst. Typically, a null will be a character which decrypts to obvious nonsense at the end of an otherwise intelligible phrase. In a **null cipher**, most of the characters may be nulls [5, 6].

This is a concealment cipher. First letters, last letters, the second letter of each word, a sequence of letters such as first-second-third, first..., letters following each vowel, etc., are some of the great variety of ways a null cipher may be constructed.

T**H**E GR**E**AT O**L**D PUM**P**ERS. In this example, the middle letter of each word is used to encipher the plaintext message reveals "HELP."

Example: Null cipher hides message in the text of another message, such as messages sent by Germans during WW I.

First letter of each word:

PRESIDENT'S **E**MBARGO **R**ULING **S**HOULD **H**AVE **I**MMEDIATE **N**OTICE. **G**RAVE SITUATION
AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

Second letter of each word:

A**P**PARENTLY N**E**UTRAL'S P**R**OTEST I**S** T**H**OROUGHLY D**I**SCOUNTED A**N**D I**G**NORED.
ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGTABLE OILS.

Reveals PERSHING SAILS FROM N.Y. JUNE 1

3.3 Spam Mimic

"SPAM" mail is the practice of sending massive amounts of unsolicited e-mail promotions or advertisements and scams to computer users. SPAM can contain identity-theft components such as "phishing" and other scams.

The spam mimic site provides access to a program that will encrypt a short message into spam. Basically, the sentences it outputs vary depending on the message being encoded. The URL is www.spammimic.com. A short message such as the geographical notations of longitude and latitude along with a Julian date might look like 39.3 N 76.6 W 170/07 could be the location of some meeting or attack. The resulting spam would look like the following e-mail message:

"Dear E-Commerce professional; This letter was specially selected to be sent to you . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail! This mail is being sent in compliance with Senate bill 1916, Title 2 , Section 309 . THIS IS NOT A GET RICH SCHEME. Why work for somebody else when you can become rich inside 58 days! Have you ever noticed more people than ever are surfing the web plus how many people you know are on the Internet. Well, now is your chance to capitalize on this. WE will help YOU deliver goods right to the customer's doorstep & process your orders within seconds! You are guaranteed to succeed because we take all the risk. But don't believe us . Ms Jones who resides in North Carolina tried us and says "My only problem now is where to park all my cars"! We are a BBB member in good standing! If not for you then for your loved ones - act now! Sign up a friend and your friend will be rich too! Thank-you for your serious consideration of our offer. Dear Business person, You made the right decision when you signed up for our mailing list ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail. This mail is being sent in compliance with Senate bill 2316; Title 1 , Section 302 ! This is a legitimate business proposal. Why work for somebody else when you can become rich within 55 MONTHS. Have you ever noticed the baby boomers are more demanding than their parents & nobody is getting any younger! Well, now is your chance to capitalize on this. WE will help YOU process your orders within seconds and use credit cards on your website! You are guaranteed to succeed because we take all the risk! But don't believe us. Mr Ames of Illinois tried us and says "Now I'm rich, Rich, RICH". We assure you that we operate within all applicable laws. We BESEECH you - act now. Sign up a friend and you'll get a discount of 60%. Cheers!"

Cutting and pasting this e-mail document into spam mimic and using decode would reveal the secret transmission.

3.4 Least Significant Bit (LSB) Substitution

One type of Steganography uses the low-order bit of the data for each pixel in an image to carry the information of a covert channel: these bits carry the covert message, while the

rest of the bits carry the legitimate image. The very slight change in the image caused by modification of the low-order bit in each pixel is imperceptible in most cases to anyone who isn't already looking for such a change.

A steganography system that uses only the low-order bit of every pixel has a low bandwidth (compared to the bandwidth consumed by transmission of the image itself), but is very discreet. A steganography system that uses all but the highest-order bit of each pixel has very high bandwidth -- but will be instantly obvious to anyone looking at the image used to carry the covert channel. Steganalysis is the art of discovering and rendering useless covert messages [5].

• LSB substitution overwrites the least significant bit of target bytes
• Example: Hide "G" (01000111) in 3 pixels – 24 bit representation of red, green, & blue

Original data
10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

Stego data
1001010**0** 0000110**1** 1100100**0**
1001011**0** 0000111**0** 1100101**1**
1001111**1** 0001000**1** 11001011

Note that only 50% of the stego bits actually change! This change would be imperceptible to most viewers.

3.5 TCP/IP Issues

TCP/IP header information can be manipulated in such a way as to encode ASCII values for transmission to outside sources. Other areas of exploration where this information can be contained are varied and include such items as ICMP (PING) packets, routing control information, and user datagram protocol (UDP) datagrams.

In the case of TCP/IP, there are a number of methods available whereby covert channels can be established and data can be surreptitiously passed between hosts. These methods can be used in a variety of areas such as the following:

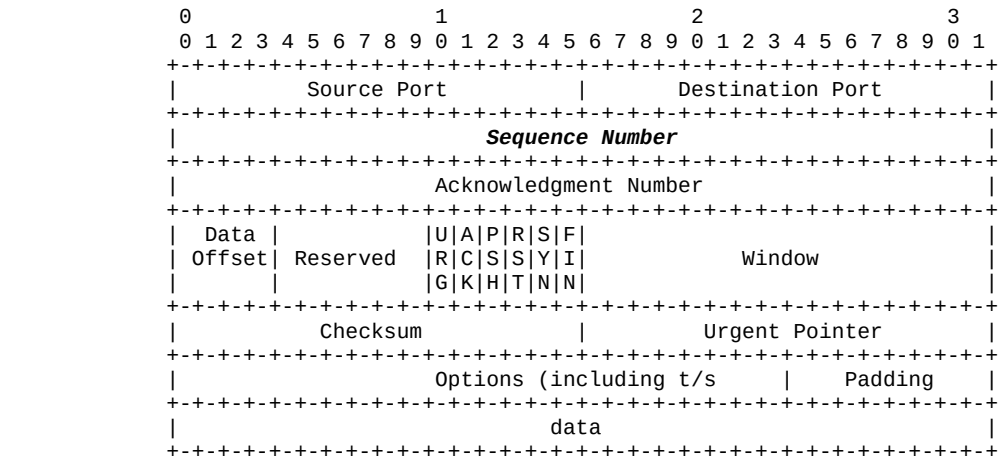
- Bypassing packet filters, network sniffers, and "dirty word" search engines
- Encapsulating encrypted or non-encrypted information within otherwise normal packets of information for secret transmission through networks that prohibit such activity
- Concealing locations of transmitted data by "bouncing" forged packets with encapsulated information off innocuous Internet sites

The TCP/IP header can serve as a carrier for a Stego covert channel if a header field can take one of a set of values which appear plausible [7]. Figure 2 highlights these carrier fields. TCP/IP exploits the fact that few headers are altered in transit, thus ensuring the transport of both legitimate and illegitimate transmissions. The TCP/IP header fields that can be used to embed Stego data include the following:

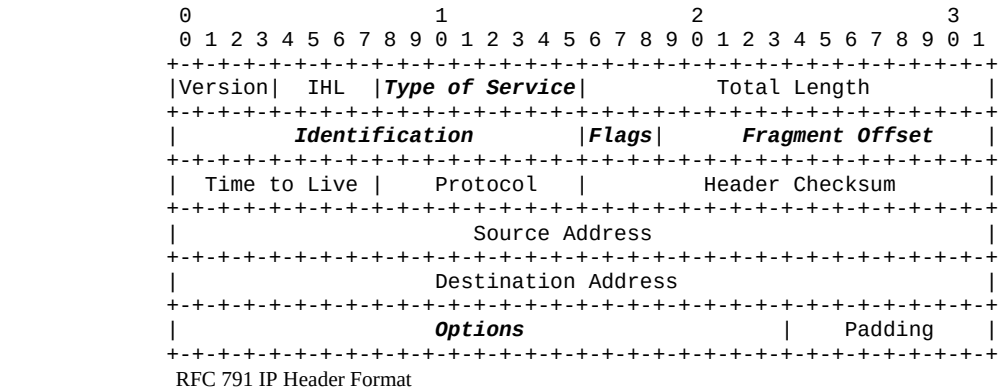
- Type of Service
- IP Identification
- IP Flags
- IP Fragment Offset
- IP Options
- TCP Sequence Number
- TCP Timestamp
- Packet Order

01001110010011110100111101000010010101000011010010000100110001001010010001100101111010101100100101010001010010000100110001001111010101000100100001001100010011110101011001001010010101000101001001001011010010100101110001011000100100001001110010110 (26 ASCII)

There are, however, procedures and tools that allow for the detection of anomalies in the TCP/IP header.



RFC 793 TCP Header Format



RFC 791 IP Header Format

Figure 2 TCP/IP Header Formats

3.6 HyperTextMarkupLanguage (HTML)

HyperTextTransportPortocol (HTTP) is used to transmit Web pages across the Internet. Simple HTML coding techniques can embed secret messages in the Web page. Encrypted comment statements can also be used to convey information; however this approach is not invisible and would cause suspicion. The secret message would not be visible unless the receiving party displays the source code. An example follows:

<html>
<body>
<head>
<title>Covert Channel Forensics</title>
This is an example of Stego!
<input type = "hidden" name = "message" value = "This is the hidden message">
</body>
</html>

4. STEGANOGRAPHY METHODS AND TOOLS

There are numerous free and commercial stego tools available for use on Windows, UNIX, Linux, MAC, and DOS systems. The primary carrier files are image and audio formats and any type of binary file can be hidden. Steganography works best in cover files with bright colors and high volume. A representative sample of tools that can hide information in various carriers (covers) includes the following [2]:

4.1 MP3Stego

This software will hide information in MP3 files during the compression process. The data is first compressed, encrypted and then data hidden in the MP3 bit stream. Although MP3Stego has been written with Stego applications in mind it might be used as a watermarking system for MP3 files.

4.2 S-Mail

It uses strong encryption and compression to hide data in EXE and DLL files. Includes a hiding scheme to ensure it is not detected by pattern and ID string scanners.

4.3 Invisible secrets

This software hides data in banner adds that appear on Web sites. Users can hide and encrypt data into a JPEG, BMP, or PNG carrier file. It includes strong encryption, FTP support, temp file wiping, and fake message generation.

4.4 Snow

It hides data within a raw text file. It does this by adding tabs and spaces to the end of lines of text. The program is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

4.5 S-Tools

S-Tools hide files in BMP, GIF, and WAV files using LSB overwriting (password used for LSB randomization and encryption). The tool will encrypt a secret message and embed into a file. Users open up a copy of S-Tools and drag pictures and sounds across to it. To hide files just drag them over open sound/picture windows. Multiple files can be hidden in one sound/picture and data is compressed before being encrypted, then hidden.

4.6 Gif-It-Up

Designed for lossless compression; hides information inside GIF files using
LSB overwriting and possesses a data encryption option.

4.7 JP Hide-&-Seek

Designed for lossy compression; hides information inside JPEG files using LSB overwriting and possesses encryption capabilities. Hides files in such a way to make it impossible to know the host file contains a hidden file.

4.8 Camouflage

Program that allows hiding files by scrambling them and then attaching them to the end of the file of choice. The file can be stored or emailed without attracting attention, however file size will increase. Password protection is included.

4.9 OutGuess

This is a universal stego tool that allows insertion of hidden data into the redundant bits of data sources. The program extracts redundant bits and writes them back after modification. The version supports both PNM and JPEG image formats. Supposedly is undetectable by Stegdetect.

4.10 EzStego

Works well with grey scale images and images with related colors. It arranges the palette to reduce the occurrence of adjacent index colors. It is a GIF-based tool written in the platform-independent Java language.

4.11 Steghide

Steghide embeds the secret message in a cover file using LSB insertion method to add more security. The information to be hidden is encrypted and pseudo randomly spread in the stego object. It can embed data in JPEG, BMP, WAV, and AU files. It provides Blowfish encryption, with 128 bit hashing of pass phrases and pseudo-random distribution of hidden bits in the container data.

4.12 Contraband

It uses the LSB insertion method to insert 3 bits of data in the LSB of each byte of the 24 bit pattern used to represent a pixel. It embeds and extracts any conceivable file.

4.13 FFEncode

It hides data in a Morse code of null characters. It uses TXT carrier files. For example:

--. --- --- -.. .--. .-.. .- -.-. . ..-. --- .-. .- -.-. --- …- . .-. - --- . … … .- --. .

4.14 Hydan

This software conceals a message into an application. It exploits redundancy in the i386 instruction set by defining sets of functionally equivalent instructions. It then encodes information in machine code by using the appropriate instructions from each set.

5. SUSPECTING COVERT TRANSMISSIONS

Why would anyone suspect covert transmissions are being made across the network? A program of monitoring the obvious carriers that could support covert transmissions is a good start. Stego software might not be located on the system as most stego software can be run without being invasively installed and fit on a memory key. There are a number of suspicion factors that should prompt further investigation. A system that contains numerous image and audio files provides carriers for covert activities. If a computer forensic analysis of an incident produces evidence of a sex crime, fraud, identity theft, child porn, drugs, gambling, hacking, smuggling, or cyber stalking incidents; covert activities might be ongoing.

A computer forensic analysis might provide hard evidence that covert channels can or are being used in the network. A partial list of some items of evidence that should raise a red flag follows:

- Stego software (or remnants) installed; registry entries
- Web history suggests visits to stego hot sites
- E-mail history shows stego purchases
- IRC/IM logs shows visits to stego/crypto chat rooms or topics
- Duplicate image/audio files found with different hash values
- Powerful Hardware
- High-end processor
- Large RAM capacity
- Graphics accelerator
- 32-bit audio hardware
- High-speed network Connection
- Powerful Software
- Image and audio processing/management tools
- Development software
- Binary editors
- Disk wiping software
- Anonymous e-mail and/or multiple online identities
- Specialized chat software

- Carrier Sophistication
- Large volume of suitable carrier files - image and audio
- Duplicate similar carrier files - image and audio
- Consistency of multimedia files by type, source, and/or encoding

6. COUNTERMEASURES

Responses when identifying covert channels can include auditing, reducing the channel capacity, and closing the channel. Auditing a channel occurs after the fact and analysis of audit data is time consuming. Reducing a channel capacity can also impact the normal, acceptable performance of the system. The only surefire solution is to restructure the channel to eliminate the security flaw. Administrators can monitor communication traffic flowing over the channels and attempt to detect suspicious activity. Channels that indicate security flaws can be closed through filtering. Policies can be instituted that allow only legitimate communications [8]. There are a number of vendors and organizations that supply tools and information which address these security flaws.

6.1 Steganography Analysis and Research Center (SARC)

The Steganography Analysis and Research Center (SARC) is a Center of Excellence within Backbone Security focused exclusively on steganography research and the development of advanced Steganalysis products and services. The SARC has developed state-of-the-art steganography detection and extraction capabilities that address the needs of digital investigation specialists and information technology security personnel in law enforcement, government, military, intelligence, and the private sector. By providing a national repository of steganography application hash values, or fingerprints, and developing the most advanced tools, techniques, and procedures to find and extract hidden information, the SARC is rapidly evolving into a high-value asset to computer forensic examiners who wish to conduct steganalysis on seized media. The SARC has products and support that can provide state-of-the-art solutions and benefits. A major product of the SARC is the Steganography Application Fingerprint Database (SAFDB).

6.2 Steganography Analyzer Artifact Scanner (StegAlyzerAS)

StegAlyzerAS gives computer forensic examiners the ability to scan either the entire file system, or individual directories, on the suspect storage media or EnCase, Raw(dd), or SMART-formatted images of the suspect storage media for fingerprints (hash values) of steganography application artifacts (files associated with steganography applications). This forensic tool offers the option to search the Windows Registry to determine if any Registry keys exist that are associated with particular steganography applications.

6.3 Steganography Analyzer Signature Scanner (StegAlyzerSS)

The Steganography Analyzer Signature Scanner is a digital forensic analysis tool designed to extend the scope of traditional digital forensic examinations by allowing the examiner to scan files on suspect media, or forensic images of suspect media, for unique hexadecimal byte patterns, or known signatures, left inside files when particular steganography applications are used to embed hidden information within them. StegAlyzerSS extends the signature scanning capability by also allowing the examiner to use other techniques for detecting whether information may have been appended to, or hidden within, potential carrier files.

6.4 WetStone Technologies

The steganography course offering provides investigators with a deep understanding of the threat posed by the use of Stego along with tools and techniques necessary to investigate Stego incidents. The course discusses the tools used by criminals exploiting children, terrorists, and intellectual property theft and crime organizations. Students learn how criminals create covert communication channels, and how disgruntled employees can easily transmit proprietary information outside the company. Students also learn how to conduct a complete Stego investigation. Each student receives a fully licensed copy of Stego Suite™ and Gargoyle Investigator™ Forensic Pro.

6.5 Stegdetect

Stegdetect is an automated tool for detecting Stego content in images. It is capable of detecting several different Stego methods to embed hidden information in JPEG images. Currently, the detectable schemes are JSTEG, JPHIDE, invisible secrets, outguess 01.3b, F5, appendX, and camouflage. Stegbreak is used to launch dictionary attacks against JSteg-Shell, JPHide and OutGuess 0.13b. Stegdetect and Stegbreak have been developed by Niels Provos.

6.6 Stego Suite (Stego Analyst, Stego Break, Stego Watch)

Programs apply statistical methods on suspect files to determine probability that Stego was employed, a guess as to the algorithm employed, and attempts to break the password. They include paletted images such as BMP, GIF, and PNG, and true color images like 24-bit BMP files and lossy compressed images such as JPG. It also includes detectors that attack audio wav file embedding.

6.7 PixAlert®Enterprise

The package is a unique image detection and analysis solution that provides active compliance to organizational policies on inappropriate and illegal content. PixAlert enables organizations to effectively manage employee computer use while reducing security and legal risks, improving IT resource management, and enhancing productivity. PixAlert software monitors and controls the viewing of illicit and inappropriate content on corporate networks.

7. SUMMARY

Use of steganography for nefarious purposes is very real! Some examinations have found a large number of "suspicious" images at eBay and 2600.com. Terrorist organizations, including Al Qaeda, are known to use forms of stego. Most law enforcement agencies don't believe that stego is being widely

used, but they don't know what they can't see or find. This is because of limited standardized processes, few tools, and lack of training.

Stego and other covert channel mechanisms can be used to leak data or provide a means to conceal it. Covert threats must be addressed according to their impact on confidentiality, integrity, and availability (CIA) of network resources and assets. The issue that does exist for information security are the threats that are “under the radar” of most systems personnel, therefore enhancing the potential risk of a surprise attack.

Security can be expressed in terms of three components, namely protection, detection, and reaction. Security personnel must monitor those assets that need protection. The key element is fast detection. Reaction to some covert channel attack is too late and often expensive!

The possibility of covert channels cannot be completely eliminated, although it can be significantly reduced by careful design and analysis. There will always be some unused portion of the bandwidth of a legitimate communications channel that can be diverted to provide a covert channel.

Stego software and carrier files have been identified for locating hidden data; however without the pass phrase, investigators may still be out of luck!

8. REFERENCES

[1] *A Guide to Understanding Covert Channel Analysis of Trusted Systems*. National Computer Security Center, Ft. Meade, Md. 20755. November 1993.

[2] Covert Channels. INFOSEC Technologies, LLC. www.infosec-technologies.com/covert.htm. Retrieved 3/14/2007.

[3] Giana, Annarita, Berk, V.H., Cybenko, G.V. *Data Exfiltration and Covert Channels*. Thayer School of Engineering, Dartmouth College. Hanover, NH. 03755.

[4] *Handbook for the Computer Security Certification of Trusted Systems*. Chapter 8: Covert Channel Analysis. Naval Research Laboratory, Washington, DC. 20375. Feb. 12, 1996.

[5] Kessler, Gary C. An *Overview of Steganography for the Computer Forensics Examiner*. Forensic Science Communications. Vol. 6, No. 3. July 2004.

[6] Kessler, Gary C. *An Overview of Steganography for the Computer Forensics Examiner*.
Computer & Digital Forensics program. Champlain College. Burlington, VT. 05446.

[7] Murdoch, Steven J., Lewis, S. *Embedding Covert Channels into TCP/IP*. University of Cambridge Computer Laboratory. Cambridge, UK. July 29, 2995.

[8] Owens, Mark. *A Discussion of Covert Channels and Steganography*. SANS Institute 2002. March 19, 2002.

[9] Smeets, Marc, Koot, M. *Covert Channels*. University of Amsterdam. Feb. 15, 2006.