
Annual ADFSL Conference on Digital Forensics, Security and Law

2007
Proceedings

# Defending Against Insider Use of Digital Steganography

James E. Wingate
*CISSP-ISSEP, CISM, IAM, Backbone Security*, jwingate@backbonesecurity.com

Glenn D. Watt
*CISSP, CISM, IAM, IEM, Backbone Security*, glenn.watt@backbonesecurity.com

Marc Kurtz
*CISSP, Backbone Security*, mkurtz@backbonesecurity.com

Chad W. Davis
*CCE, Backbone Security*, chad.davis@backbonesecurity.com

Robert Lipscomb
*Backbone Security*, robert.lipscomb@backbonesecurity.com

# Defending Against Insider Use of Digital Steganography

**James E. Wingate, CISSP-ISSEP, CISM, IAM**
Backbone Security
jwingate@backbonesecurity.com

**Glenn D. Watt, CISSP, CISM, IAM, IEM**
Backbone Security
glenn.watt@backbonesecurity.com

**Marc Kurtz, CISSP**
Backbone Security
mkurtz@backbonesecurity.com

**Chad W. Davis, CCE**
Backbone Security
chad.davis@backbonesecurity.com

**Robert Lipscomb**
Backbone Security
robert.lipscomb@backbonesecurity.com

## ABSTRACT

The trusted insider is among the most harmful and difficult to detect threats to information security, according to the Federal Plan for Information Assurance and Cyber Security Research and Development released in April 2006. By default, employees become trusted insiders when granted the set of privileges needed to do their jobs, which typically includes access to the Internet. It is generally presumed the insiders are loyally working to achieve the organization's goals and objectives and would not abuse the privileges given to them. However, some insiders will inevitably abuse some of their privileges. For example, a trusted insider might abuse their privilege of access to the Internet to download, install, and use an information hiding tool, such as one of the hundreds of digital steganography applications available on the Internet, to steal sensitive, classified, or proprietary information. Effective countermeasures to this threat must begin with an organizational policy prohibiting installation of information hiding tools on user workstations and must also include automated tools capable of detecting attempts to download and use digital steganography applications. This paper will describe the threat from insider use of digital steganography applications; a new approach to detecting the presence or use of these applications; and extraction of hidden information when a known signature of one of these applications is detected. The analytical approach to steganalysis involves the development and use of computer forensic tools that can detect "fingerprints" and "signatures" of digital steganography applications. These tools can be employed in both an off-line forensic-based mode as well as a real-time network surveillance mode. Detection of fingerprints or signatures in either mode may lead to the discovery and extraction of hidden information. Accordingly, this approach represents a significant improvement over traditional blind detection techniques which typically only provide a probability that information may be hidden in a given file without providing a capability to extract any hidden information.

**Keywords:** insider, steganography, steganalysis, computer forensics, artifacts, fingerprints, hash values, signatures

## 1. THE INSIDER THREAT

When considering the magnitude of the insider threat, it is instructive to consider the *Hard Problem List* (HPL) composed by the Information System Security (INFOSEC) Research Council (IRC) (IRC, 2005). The HPL is a list of eight problems considered to be the hardest and most critical challenges to building, deploying, and operating trustworthy systems. The *Insider Threat* is number two on the list.

In describing vulnerabilities, threats and risk, the Federal Plan for Cyber Security and Information

Assurance Research and Development released in April, 2006 lists insiders as an example of a threat agent along with the usual threat agents such as malicious hackers, organized crime, terrorists, and nation states (NITRD, 2006). Further, in describing threat and vulnerability trends, insiders are at the top of the list.

Another currently popular way to gauge the level of interest in a particular topic is to "Google" it. Running a Google search on "insider threat" returns 302,000 links; indicating a significant level of interest in the topic.

Some authors subdivide insiders into two groups: presumably "regular" insiders and another group of "trusted" insiders (IRC, 2005). The criteria for being a member of the trusted insider group is that members of this group possess significantly more technical ability than do the members of the regular insider group. For example, software developers and system administrators would be considered trusted insiders.

The term "trusted insider" implies there are insiders that are not trusted. While, in reality, it is true that all insiders cannot be trusted, the creation of an account with a userid and password is an explicit indication of a trust relationship between the organization and the insider. Thus, the use of "trusted" with "insider" is redundant.

The Federal Plan previously mentioned also lists the use of cyberspace for covert communications right after physical attacks against key data centers and communications nodes on the list of immediate concerns for the U.S. IT infrastructure (NITRD, 2006).

The means to accomplish covert communications is readily available to insiders in the form of digital steganography applications that can be used to hide information inside of digital files in such a way the hidden information cannot be seen or heard by normal human senses and is extraordinarily difficult to detect even when looking for it with state-of-the-market automated detection tools and techniques.

A Google search on "steganography" returns 1,720,000 links which speaks volumes about the level of interest in this topic.

To make matters even worse, encryption can be, and often is, used in conjunction with steganography. This makes a formidable challenge even more formidable because the hidden information must not only be detected and extracted; it must also be decrypted if it was encrypted prior to being hidden.

Accordingly, as an enabling technology for U.S. adversaries, use of steganography has significant implications for U.S. national security (NITRD, 2006). Because steganography can be used to steal intellectual property, it also has significant implications for U.S. economic security.

## 2. DIGITAL STEGANOGRAPHY

Secret communication, in one form or another, has been used throughout history. *The Codebreakers* by David Kahn provides an excellent treatment of this topic by interleaving the history of both steganography and cryptography (Kahn, 1996).

Fast forwarding to the Internet era, steganography manifested itself in the form of "digital steganography" which generally involves hiding a binary file inside of another binary file, typically called the carrier file. Although there are many ways to hide information inside practically any binary file (Kessler, 2004; Arnold et al., 2003; Bauer 2002), image and audio files are the most common carriers in use today. Typically, text files and image files are hidden inside other image files and text files are also hidden inside audio files.

Information hiding through the use of digital steganography has significant implications in the following three areas:

- Law Enforcement
- Intelligence
- Industry

Law enforcement investigators and computer forensic examiners at the federal, state, and local level are encountering and ever increasing number of cases that involve the seizure, preservation, and analysis of digital evidence. Digital steganography can be used to conceal evidence of criminal activity and, perhaps of more concern, can be considered an effective anti-forensic tool because the current generation of computer forensic tools does not detect the presence or use of digital steganography.

On their list of counter-surveillance technologies, intelligence agencies must be concerned about the use of steganography to defeat state-of-the-art surveillance tools and techniques to conceal evidence of terrorist activity.

Finally, private sector companies with significant amounts of intellectual property to protect must be concerned about the use of steganography by insiders as a means to steal their crown jewels. The electronics and pharmaceutical industries, in particular, come readily to mind.

It is sobering to think of what might be hidden in the billions of images floating around on the Internet every day and on the millions of portable audio devices in use world-wide that collectively contain billions, and possibly trillions, of audio files. Then, the potential for hiding information on the millions of computers on enterprise networks and personal computers in homes must also be considered.

## 3. DIGITAL STEGANALYSIS

Steganalysis is somewhat analogous to cryptanalysis. The objective of cryptanalysis is to reverse the cryptographic process to reveal the plain text. However, an additional step is required with steganalysis. The hidden information must first be detected. Then, the objective becomes reversing the steganographic process to reveal the hidden information. After the hidden information is revealed, or extracted, the examiner may find the extracted information is cipher text, indicating the information was encrypted prior to being hidden in the carrier file. Depending on how much is known about how the application encrypted the payload and whether or not the user-supplied password was embedded in the carrier file along with the payload and whether that password can be cracked or replaced with a null password, classis cryptanalysis may be necessary to attempt to decrypt the hidden information.

The first step, then, is to determine if information has been hidden in the carrier file. This is often referred to as detecting the payload.

Much research has been done since the mid- to late-1990 timeframe on techniques for detecting payloads in carrier files. Most of that research has been focused on a technique typically referred to as "blind detection."

There are three classical "attacks" employed when using the blind detection technique (Kessler, 2004):

- Visual
- Structural
- Statistical

Each of these attacks result in varying degrees of success in determining whether or not a suspect carrier file contains a hidden payload. Typically, automated blind detection algorithms that perform structural and/or statistical attacks yield only a probability that information has been hidden in the carrier file with limited, if any, capability to attempt to extract the hidden payload.

A probability that hidden information may exist in suspect carrier files may be sufficient in some cases. For example, in an intelligence "man-in-the-middle" surveillance scenario, a high probability

that information has been hidden in suspect files could provide the opportunity to alter the file such that the hidden message is scrambled such that the original message does not make it to the intended recipient.

For law enforcement purposes, however, a probability that information may be hidden in a file is generally insufficient. Law enforcement computer forensic examiners must be able to both detect and extract hidden information in order for the investigator to have information of potential evidentiary value to present to a prosecutor. It is inconceivable that any prosecutor would be willing to file charges against a suspect based on an investigator's assertion the suspect "may have hidden" evidence of criminal activity in files on the suspect's computer.

Accordingly, steganography represents a technology that hampers law enforcements' ability to conduct successful investigations where suspects have used digital steganography as an anti-forensics tool that makes it exceedingly difficult, if not impossible, to find digital evidence.

In a national needs assessment for law enforcement tools and technologies conducted in 2002 by the Institute for Security Technology Studies (ISTS) at Dartmouth College, steganography is described as presenting "immediate and long-term challenges for law enforcement" (ISTS, 2002). Assessment participants also called for "a clearinghouse of digital steganographic programs and signatures that could be consulted during forensic analysis of a seized computer." Finally, the assessment concluded the section on steganography by stating the need for "additional long-term research into breakthrough technologies for steganography detection."

The previously referenced Federal Plan (NITRD, 2006) concluded the section on steganography by stating that advanced methods for detecting steganography need to be developed and deployed to detect covert communications along with a recommendation to enhance resources "to evaluate, integrate, and deploy" basic research advances in the evolving field of digital steganalysis.

## 4. AN ANALYTICAL APPROACH TO STEGANALYSIS

Due to limitations inherent in the blind detection approach to steganalysis, a new and improved approach is needed.

Rather than looking blindly at suspect carrier files, this paper suggests it would be much more productive to take a more analytical approach to the problem that involves searching for the ***fingerprints*** and ***signatures*** of steganography applications.

An excellent indication that a steganography application may have been used to hide information would be detecting the presence of a steganography application on a seized computer. Much like the popular baseball movie "Field of Dreams," where the premise for achieving a gathering of the most famous ballplayers of all time, was to "Build it, and they will come," the premise for detecting the presence of a steganography application is "If its there, it was used." This premise can be extended to include "if it was used, it was used to hide something."

Two key questions then result from the initial and extended premise … "what was hidden and where was it hidden." The task for the examiner then becomes on of focusing their examination on finding where the information might have been hidden; then find it and extract the hidden information.

The presence of a steganography application can be detected by scanning suspect media for the "fingerprints," or hash values, of "artifacts" of the steganography application. An artifact is a file, or several files, resulting from the installation of a steganography application. A more detailed description of artifact detection follows, but first a more in dept discussion of fingerprints is necessary.

The fingerprint is a hash value of a file artifact. Hash values, often referred to as a Message Digest, have traditionally been computed using either the CRC-32, MD5, or SHA-1 algorithms. It is computationally infeasible, in theory anyway, to find two different messages that produce the same message digest. And, given any message digest, it is not possible to reverse the hashing process to

obtain the original message. Accordingly, the term "one way hash" is often used to convey the irreversibility of the process.

In February, 2004, the National Institute of Standards and Technology released the Secure Hash Standard (SHS) that added three additional algorithms capable of producing larger message digests for digital signatures and message authentication (NIST, 2004). The new standard added the SHA-256, SHA-384, and SHA-512 algorithms. A subsequent change to the SHS added the SHA-224 algorithm. Thus, at the present time, there are seven different algorithms that can be used to generate the fingerprint of a file artifact: CRC32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

An excellent indication that a steganography application was used to hide information would be detecting the "signature" of a steganography application. Extensive research on selected steganography applications, to be described in a subsequent section, has resulted in the discovery that some steganography applications leave a uniquely identifiable signature, or hexadecimal byte pattern, in a carrier file.

The use of a steganography application can be detected by scanning all the files on suspect media for known signatures of steganography applications. This should not be done until traditional forensic file recovery tools and techniques have been run to recover deleted files, files in slack space, files in swap space, etc. A more detailed explanation of signature scanning follows.

## 5. STEGANOGRAPHY APPLICATION ARTIFACT DETECTION

An ***artifact*** of a steganography application is a file or registry key added to a system as a result of installing or running a steganography application. A fingerprint is one of up to seven different hash values of a file artifact. Registry artifacts are applicable only to Windows platforms because the concept of a Registry is unique to Microsoft operating systems. File artifacts exist for steganography applications that run on numerous other operating systems such as Macintosh, Linux, Amiga, OS2, AIX, HPUX, Solaris, and even Symbian.

Scanning the file system on seized media for fingerprints of file artifacts, and registry artifacts for Windows platforms, enables the computer forensics examiner to determine if a particular steganography application is currently on the media or was at one time. Many artifacts can be easily removed from a system by uninstalling the associated steganography application and then deleting the obvious files and folders not removed during the uninstall process. However, it is important to remember that some number of file and registry artifacts, referred to as ***residual artifacts***, may remain on the system in spite of user attempts to cover their tracks. Residual artifacts can be detected by an examiner equipped with the proper tools and can serve as proof the user installed a specific steganography application at some point in time.

The investigator or examiner should interpret detection of a steganography application artifact as an indication of the user's intent to hide something with that application. Artifact detection yields a couple of questions such as "What information was hidden? and "Where was the information hidden?" It is important to be able to associate any artifact with a particular steganography application to improve the chances of finding and extracting any information hidden with the application. The examiner can then find additional information about the application by consulting repositories of steganography application research data to answer some very important questions such as:

- What types of files (i.e., carrier files) can be manipulated by the particular application?
- What type of embedding technique does this application use?
- What type of encryption, if any, does this application use?

By answering these questions, the examiner can narrow their search to a certain set of file types, possibly only one file type. Armed with specific information about the application used to hide information, the examiner has a much better chance of finding the carrier files and extracting the hidden information.

The above information provides an explanation on the basic concept of artifact detection. Depending on the type of steganography application that was used to hide the data initially, it can be a very difficult task to recover the hidden data. In many cases, if strong encryption was used to encrypt the data before it was hidden, a recovery of the hidden data may never be possible. When tackling the insider threat, this example shows us that a more proactive approach is needed in cases concerning steganography. The detection of the use of a steganography application to steal sensitive, proprietary, or classified information after the fact simply will not suffice in cases of this nature. Furthermore, it is also important to remember that an investigation after the fact will not reveal how much sensitive, proprietary, or classified information has previously been stolen by the insider. Immediate, real-time detection of the artifacts of steganography applications is the only strategy that will provide an all-encompassing solution to these types of crimes.

By monitoring the files present on an insider's machine and within their network traffic in real-time, it is possible to detect that a trusted employee is in the process of using a particular steganography application to smuggle sensitive, proprietary, or classified information outside of the workplace. Once it is determined that an artifact of a steganography application exists on, is entering, or is leaving an employee's work station, action can then be taken to either monitor this employee's actions more carefully or seek immediate disciplinary action against them.

## 6. STEGANOGRAPHY APPLICATION SIGNATURE DETECTON

Many steganography applications embed a unique hexadecimal byte pattern as a by-product of embedding hidden information within carrier files. This hexadecimal byte pattern is used by the steganography application to identify whether or not it was used to manipulate the carrier file. These signatures are verifiable and repeatable. A hit on a signature would indicate that the steganography application has been used to hide something within a carrier file.

To determine a signature for a particular steganography application, a large number of test images must be created using that application. A set of images known to be clean of steganography is used as carrier files. A set of text, image, and audio files of various sizes are used as payload files. Several combinations of the carrier and payload files are used to create a Reference Image Library. All options such as encryption and compression are used to create the set of reference images. The goal is to create as diverse a set of stego images as possible. Once created for each steganography application, the reference images are then compared to each other to identify patterns of data that can be used as signatures. Signatures can vary in length and a steganography application may have more than one signature.

Signature detection is a highly accurate method of detecting the use of steganography within a carrier file. False positive results can occur for very small signatures (one to three bytes). However, in many instances additional information can be used in correlation to verify the signature and reduce the false positive rate.

Unlike the blind detection method which gives you a probability that a particular algorithm (LSB modification, DCT modification, etc) was used to embed the hidden data, the signature detection used by the Analytical Approach pinpoints the particular application that was used to embed the hidden data. A major advantage of signature-based detection is that as a by-product of the extensive research that goes into the signature discovery process is knowledge that can be used in creating an automated extraction algorithm for recovering the hidden information.

In some cases, the passwords used to embed or encrypt the information prior to embedding can be exploited to recover the payload. Kerckhoffs' principle states that a system's security relies on key management, not the secrecy of the algorithm used (Kerckhoffs, 1883). In other words, security through obscurity is no good. It is not important that everyone knows the techniques used to embed the hidden data, rather the security of the data relies on a secret key used to protect the hidden information. Some steganography applications use strong encryption (AES, 3DES, Blowfish,

Twofish, etc.) but leave the passwords used for encryption either in plaintext or as a simple XOR. These passwords can be defeated by replacing the password with null or known passwords.

Signature detection is not a panacea or be all-end all solution for steganalysis because some applications leave no signature behind. This limitation may ultimately require the use of more traditional blind detection techniques.

## 7. REAL-TIME DETECTION OF STEGANOGRAPHY APPLICATION ARTIFACTS AND SIGNATURES

Detecting artifacts and signatures of steganography applications after the application has already been downloaded or installed and used is not unlike locking the barn door after all the horses are out.

Accordingly, a means to keep steganography applications from being downloaded, installed, and used in real-time is of paramount importance.

By placing a network security appliance that employs application proxies to intercept and reassemble HTTP and SMTP packet traffic into files, it would be possible to detect fingerprints and signatures of steganography applications.

The expected scenario would be one where an insider finds a freely available steganography application on the Internet and downloads that application onto their network connected computer. The user would then install the application and use it to hide some information in a carrier file. Then, the user would either upload the carrier file to a publicly accessible web site or send the carrier file to an external recipient as an attachment to an e-mail.

With real-time detection, the steganography application would be detected in the in-bound network traffic stream. Upon detection, the file could be logged and passed on to the user or it could be blocked and placed into quarantine for subsequent analysis or investigation. The important point is detecting any steganography application inbound should be a critical early warning indicator that an insider intends to use the application to hide something. Network security staff can then increase surveillance on the user to find out more information such as what type of information might they be trying to conceal or steal and to whom might they be intending to send it to.

If the decision is to log and pass the application to the user, it must be assumed the user will install the application, use it to hide something in a carrier file, and then attempt to exfiltrate the carrier file from the network by posting it on a web site or sending it to someone as an e-mail attachment.

Here again, real-time detection may be able to detect a signature in the out-bound network traffic. In the same way in-bound traffic is reassembled by application proxies and subsequently hashed to determine if the inbound file is an artifact of a steganography application, out-bound traffic can be reassembled and the resulting files can be scanned to determine if a known signature of a steganography application exists in the out-bound carrier file.

While the discovery of signatures of steganography applications will certainly always lag behind the discovery of artifacts, and it is very highly likely that some steganography applications will not have a signature, the combination of scanning inbound traffic for known artifacts and scanning outbound traffic for known signatures is expected to be an effective countermeasure to the threat of insider use of steganography.

Generally, the capability of all software tools improves over time. Likewise, it is expected the capability of real-time steganalysis tools will also improve over time. And, while it would be unreasonable for anyone to expect the tool would ever be able to detect all steganography application artifacts and signatures, it is very reasonable to expect the tool will detect some amount of insider use of steganography to steal sensitive, classified, or proprietary information.

## 8. BEST PRACTICE

The first step in addressing the steganography threat should be to develop and distribute a policy prohibiting users from downloading, installing, and or using steganography or any information hiding tools on the organization's networked computers. While many organizations already have an "Acceptable Use" policy that covers many topics, that may possibly include a list of prohibited software, the policy aspect may be dealt with by simply adding steganography and information hiding tools to the list of prohibited software.

After addressing the policy aspect of steganography countermeasures, the organization should identify and deploy a real-time steganography detection capability. While it would be nice if any of the currently available content filtering and Unified Threat Management (UTM) included the detection of steganography, the reality is that these tools do not do this. Accordingly, they all have a huge gaping hole in their insider threat defenses because they do not detect covert channels that can be established by insiders through the use of steganography.

Until such time as steganalysis capability is integrated into currently available, or new, content filtering and UTM tools, it may be necessary to employ a special-purpose network security appliance with the capability to detect steganography in real-time.

Ideally, the threat of insider use of steganography would be most comprehensively addressed by employing real-time and off-line steganalysis capability in tandem. The off-line detection could be performed through forensic analysis of employee computers. For example, during non-working hours, the hard disk drives on employee computers could be imaged for subsequent processing by security staff using forensic tools designed to detect fingerprints and signatures of steganography applications. This approach could detect the presence of steganography applications that had been downloaded prior to the deployment of the real-time detection capability.

While some may look-upon the forensic analysis of employee computers as an intrusive surveillance technique or as a "Big Brother" spying type activity, it should be considered in the context of configuration management. A best practice of configuration management is to know exactly what software is on each computer connected to the organization's network. If steganography applications, or any malware for that matter, are there and no one knows it, then intellectual property or other sensitive or classified information may be leaking out of the network without anyone knowing about it. This should serve as proof that the old saying "What you don't know can't hurt you" is not at all true in this digital age. Rather, what you don't know can hurt you … and the pain can be immeasurable in terms of financial loss as well as the impact on U.S. national, homeland, and economic security.

## 9. CONCLUSIONS

In the words of Tom Clancy, digital steganography is a "clear and present danger." It is a significant threat but nobody really knows how much it's being used because no one is looking for it.

A paradigm shift in the field of computer forensic examination is needed to adequately address this threat. Computer forensic examiners should include steganalysis as a routine aspect of their examinations much like the recovery of deleted files and the search for information in swap space and slack space is done routinely.

Steganalysis should always be performed in the laboratory environment and on a case-by-case basis when doing field triage (Debrota, S., Goldman, J., Mislan, R., Rogers, M., and Wedge, T., 2006). It is not difficult to envision scenarios where an examiner may not find any information of value in a field triage but a quick steganography artifact scan may reveal the suspect used a steganography application as an anti-forensic tool to conceal key evidence. That may, in turn, help the examiner find information of value hidden in carrier files on the media being examined in the field or may help to focus a subsequent laboratory examination to find hidden information more quickly than it otherwise may have been found.

Private sector companies with significant amounts of intellectual property to protect should be very concerned about the threat posed by insider use of steganography to steal their intellectual property and should employ effective countermeasures as soon as practical because the content filtering and UTM tools they may have deployed do not detect the presence or use of steganography.

For law enforcement and private sector computer forensic examiners to have the capability to routinely scan for fingerprints and signatures of steganography applications, a national repository of steganography applications, fingerprints and signatures is needed. This need was listed in the ISTS National Needs Assessment (ISTS, 2002). Keeping the repository populated with newly developed or discovered steganography applications will be an on-going and long term need.

Additionally, computer forensic examiners will also need state-of-the-art tools to detect the presence and use of steganography applications to conceal evidence of criminal activity. After detecting hidden information, the examiners will need the automated tools necessary for extracting the hidden information because a manual extraction process is much too time consuming and onerous to expect even the most dedicated and technically proficient examiners to perform.

Finally, research to advance the state-of-the-art of steganalysis must be continued. Much research has been done in the area of hiding text and image files inside of other image files, although much more needs to be done. However, much less research as been done in detecting hidden information in audio and video files. The exploding number of mobile personal computing, audio, and video devices has resulted in the existence of billions, if not trillions, of audio and video files—each of which can serve as a carrier file for hidden information.

Refusing to believe, or even consider, that steganography is being used is "security through denial" and that will never provide any assurance that sensitive information isn't leaking out of the network like a sieve.

Steganography will never be found if no one ever looks for it. In the meantime, large amounts of digital evidence of criminal activity may be going undetected.

## 10. REFERENCES

Arnold, M., Schmucker, M., and Wolthusen, S. D. (2003). Techniques and Applications of Digital Watermarking and Content Protection. Artech House, Norwood, Massachusetts.

Bauer, F. L. (2002). Decrypted Secrets: Methods and Maxims of Cryptology, 3rd. ed. Springer-Verlag, New York.

Debrota, S., Goldman, J., Mislan, R., Rogers, M., and Wedge, T. (2006). *Computer Forensics Field Triage Process Model*, Proceedings of the Conference on Digital Forensics, Security, and Law 2006 (pp. 27-36), Las Vegas, Nevada, April 20-21, 2006.

Homer-Dison, T. (2002). The Rise of Complex Terrorism. Foreign Policy, 128, 52-62. Retrieved from http://www.foreignpolicy.com/story/cms.php?story_id=170.

INFOSEC Research Council (IRC). (2005). *Hard Problem List*. Retrieved from http://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf.

Institute for Security Technology Studies (ISTS), Dartmouth College. (2002). Law Enforcement Tools and Technologies for Investigating cyber Attacks: A National Needs Assessment. Retrieved from http://www.ists.dartmouth.edu/TAG/lena.htm.

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Revised ed., Scribner, New York, 1996.

Kerckhoffs, A. (1883). *La cryptographie militaire*, Journal des sciences militaires, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.

Kessler, G. C. (2004). An Overview of Steganography for the Computer Forensics Examiner. Retrieved from http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm.

Networking and Information Technology Research and Development (NITRD) Subcommittee of National Science and Technology Council (NSTC) Committee on Technology. (2006). *Federal Plan for Cyber Security and Information Assurance Research and Development*, April 2006. Retrieved from http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf.

National Institute of Standards and Technology (NIST) Computer Security Division. (2004). Federal Information Processing Standard 180-2, Secure Hash Standard (SHS). February, 2004. Retrieved from http://www.csrc.nist.gov/publications/fips/index.html.