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

Steganography- See No Evil, Hear No Evil, Speak No Evil.

Chris Farrow
GSEC Practical v1.3
May 13th, 2002

Abstract

With the world focused on terrorism propagated by poor security and businesses suffering from huge economic losses due to computer crime, information security has become a top focus of IT departments. Corporations have begun to heavily implement strategies to secure their workplaces and the information associated with their business. Security tradeshows have sprung up around the globe and organizations are spending significant portions of their budget on training and outsourcing.

Yet, despite this revival in information security there are still entire fields of security that remain virtually unknown. Of these, steganography provides not only an exemplary tool for protection of intellectual property and a medium of private communication but also a serious risk to the security of an organization. Amazingly, a simple search of online stores for steganography books and courses finds this subject to be almost unheard of. Further research for steganographic focused vendors shows there is a serious lack of strategy and defensive solutions for the corporate world.

This paper is intended to explore the legitimate and malicious uses of steganography and the lack of defensive strategies to counter steganographic techniques. To adequately understand the subject material, the paper provides background information on the history of steganography, an overview of different types of steganography and popular steganographic tools.

Definition of Steganography

Steganography, as defined by Webopedia [1], is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Originating back to the ancient times, the term steganography is derived from the Greek word *steganos*, meaning covered or hidden, and *graphy,* meaning writing. In our computerized civilization, steganography has expanded to include covert inclusion of data in any other data source including text, audio, and video. It should be noted, many scholars relate steganography to cryptography. The difference is where cryptography is designed to protect the content of the message, steganography is designed to hide the fact that a message even exists. Steganalysis is the science of detecting the presence of a steganographic message.

History of Steganography

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Steganographic techniques have been used throughout history to provide a means of covert communication. The earliest written records of steganography come from the writings of Herodotus. As referenced by Katzenbeisser and Petitcolas [2], Herodotus tells of how Histiæus communicated to his son-in-law in Greece to revolt, by shaving the head of his most trusted slave and tattooing it with a message which disappeared after the hair had grown back. The slave then made his way from Persia to Greece where the message was delivered. Other methods such as using wood tablets to write the message upon and then covering the tablet with wax were also used by Demeratus to warn Sparta of an invasion by Persia.

Later, in Roman society, important messages were commonly written in invisible inks designed to hide the existence of the message. Many different liquids were used as inks including juices and urine[3]. The ink would be used to write invisible messages which could then be read when heat was applied to the writing. Today, these invisible inks are still being used by children as science projects [4].

Steganography continued to develop and be used throughout the middle ages. Several academic works on steganography were produced including *Steganographia*, by Johannes Trithemius, and *Steganographica,* by Gaspari Schotti [5]. Interestingly enough, steganography worked its way into literatures. For a long time, the works of William Shakespeare were thought by some to be penned by English writer Francis Bacon. Even though some 4000 books have been authored addressing the subject of the real identity of Shakespeare [7], in his 1990 work, The Second Cryptographic Shakespeare [6], Penn Leary uncovered steganographic evidence that indicated that Francis Bacon might have actually used William Shakespeare as merely a pen name.

In the modern era, steganography was used extensively in World War I and World War II. Invisible inks were still being used [10], but had progressed to complex chemical compounds that remained undetected unless in the presence of a second chemical. Allied Forces used coded radio broadcasts to communicate information over what sounded like normal news and entertainment programs. In World War I, the Germans invented the microdot based on research regarding microscopic image techniques published by Brewster in 1857 and microfilm techniques used in the Franco-Prussian War [13]. Per Merriam-Webster, a microdot is "a photographic reproduction of printed matter reduced to the size of a dot for ease or security of transmittal" [9]. The microdot was extremely effective for espionage as the presence of the message was difficult to detect in everyday documents.

Types of Steganography

Steganography has three major mediums: Text, Audio and Graphics. Textual steganography follows closer to the original definition as it concentrates on hidden communication through written means. Auditory steganography, which has been greatly

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

advanced by modern computing technology, utilizes conversation or music as a carrier to convey convert messages. Finally, graphical steganography is the method of hiding messages in graphic and video images, either in print or more commonly, electronic format.

As outlined by Sellars [2], textual steganography utilizes manipulation of the text itself. Text based steganography makes use of one or more of the techniques of 1) word shift, 2) line shift, 3) white space, or 4) features. Word shift involves shrinking or increasing the horizontal spacing of text while line shift changes the vertical spacing between lines on a page. White space techniques involve changing the white space between letters over an entire document. Last of all is the imperceptible tweaking of text features such as fonts and formatting.

Auditory steganography involves taking advantage of the human auditory system and its limitation. By substituting data for minute portions of the audio data (the least significant bits), a secondary message can be encoded in the original media. If done properly, the modified audio is indistinguishable from the source. Auditory steganography can also make use of code words in regular news or sports broadcasts. Listeners to a newscast would suspect nothing, but for someone in the know, a code word mentioned could have special meaning. Subliminal messages can also fall into this category. Due to the huge trafficking in MP3 traffic via peer-to-peer technologies, digital audio is one of the most readily available carriers available.

Graphic steganography has been used for thousands of years, from simple symbols drawn on buildings to next generation computer programs designed to bury information in a digital image. As the Internet has expanded and matured beyond the days of text based web browsers, the graphical nature of computing has moved from the desktop out to the web. Now that higher bandwidth is available to the typical home user, a greater use of graphic and video has become commonplace. All of these changes have provided a target rich environment in which steganography can be used to convey proprietary corporate information, secret military plans or even tools for computer criminals. JPG, GIF, BMPs, AVIs and MPGs are file formats useful for this type of steganography.

Steganographic Tools

Today, advances in computer technology and the instant information age of the Internet has made a large selection of steganographic tools and utilities available for the casual web surfer. A quick online search reveals online stockpiles of tools supporting numerous platforms including Windows, DOS, Java, Macintosh, OS/2, Unix/OpenBSD/Linux and Amiga [13].

Some examples of the more popular tools are outlined below:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Steganos 4 Security Suite is a commercial product line providing online privacy and file protection through encryption and steganography [13]. Further information can be found at http://www.steganos.com/en/index.htm.

Datamark [19] utilizes steganography to product watermarks in BMP, GIF, JPG, PDF, PNG, TIFF, TGA formatted files. Further information can be found at http://www.datamark-tech.com/datamark.html

S-Tools [17] is one of the classics in steganography utilities. *S-Tools* provides the ability to hide messages in BMP, GIF and WAV files. Optional encryption is also available. A copy of the software, with documentation is available from ftp://ftp.ntua.gr/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip

WBStego [18] is a very useful all-around tool as it supports BMP images, text files, HTML files or Adobe PDF files. The payload data can even be encrypted inside the carrier file. Further information can be found at http://wbstego.wbailer.com/.

JSTEG-Shell [13] is an excellent products for hiding information inside of JPG graphics. The products includes a command line as well as a GUI interface for the tool. *JSTEG-Shell* also includes 40 bit rc4 encryption of the payload message. Usage information with screenshots can be found at http://www.tiac.net/users/korejwa/jstegscreenshot.htm.

BMP Secrets [16] is slightly different tool that can hide a large amount of data in a BMP format graphic file. *BMP Secrets* provides a Windows GUI and built in encryption. Further information can be found at http://www.pworlds.com/products/i_secrets.html.

MP3Stego [18] has both GUI and command-line versions that hide information in MP3 files and is one of the only tools available anywhere for MP3 steganography. Further information can be found at http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego. *Texthide*[20] is a program that embeds hidden text messages in what appears to be normal text messages. This is done by making small changes in the existing text features. The hidden message can still be encrypted, even though in plain text. For further information, see http://www.compris.com/subitext/

Spam mimic[21] takes a refreshing approach by transform a text message into a never ending piece of email SPAM. SPAM mimic is offered as online service at http://www.spammimic.com/

Sam's Big Play Maker [22] is similar in concept to *Spam mimic* but instead of transforming the message into a SPAM message, the output is in the form of a senseless multi-act play. More information on this tool is at http://www.scramdisk.clara.net/play/playmaker.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Uses of Steganography: Government, Military and Intelligence agencies

While steganography is hardly mainstream in the commercial sector, steganography is not totally without supporters. The Federal Government and the Department of Defense are long time advocates of the technologies used to mask and discover covert communication. Throughout both World Wars and even into modern times, the United States and other national governments have utilized covert communications with numerous technologies including coded radio broadcasts, embedded images, messages written using invisible inks and microdots. Today, even though the cold war is over there is still heavy focus on steganography in the military intelligence community. There is suspicion that terrorists involved in the World Trade Center bombing [11] utilized steganographic messages on the Internet to layout their plans. As part of the investigation, the FBI and NSA are using all the tricks they have involving information capture and forensics, including the use of Carnivore, the FBI's packet sniffing system and Echelon, the theorized espionage network watching global communication. [23].

The Federal government has even sponsored their own research and development projects to further steganographic and steganalytic techniques. Wetstone Technologies produces steganalytic and forensics solutions that were developed as part of a joint project with the Department of Defense [24]. The U.S. Air Force grants to Binghamton University in NY are focusing on perfecting new audio and video steganographic techniques [26] and the NSA has underwritten the work of Neil F. Johnson and George Mason University's Center for Secure Information Systems [25]. Without a doubt, national governments around the globe have contributed greatly the science of steganography and steganalysis.

Uses of Steganography: Economic Espionage and Copyright Protection

The Federal government's interest in steganography has not been limited to just the military topics. In 1996, the United States passed the Economic Espionage Act of 1996, 18 U.S.C. §§ 1831- 1839 [27], The Act had two major concerns. The first outlawed the theft of economic trade secrets that would benefit a foreign government, entity or agent. The second article outlawed the commercial theft of trade secrets, purely for economic or business gain. Since the act was enabled, at least 35 cases have been brought to federal court [28] regarding the theft of trade secrets. Economic espionage has now become a serious focus of both the federal and private sectors, with books and websites dedicated to the topic[29] [43].

Outside of economic espionage, the commercial sector is being bombarded with economic challenges as well. In 2001, the Business Software Alliance (BSA) reported that software piracy is responsible for $11.8 billion in economic loss [30]. Microsoft and other vendors have worked with local authorities in Asian countries to combat mass software duplication and piracy organizations. Some reports from the BSA have shown that over 50% software in Hong Kong is from a pirated source. The problem of software

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

piracy is so rampant, that even the FBI has been brought in to help enforce the law [31]. However, as widespread as software piracy appears to be, music piracy has become the new target of law enforcement.

The late 1990s saw MP3s becoming the personal audio standard and the popularity of peer-to-peer file sharing technologies like Napster and Gnutella was at an all time high. Audio piracy quickly became the new past time of office workers and college students everywhere. Many companies and universities had to make network configuration and policy changes to keep their bandwidth from being consumed. Over the last 2-3 years, the piracy of music has ballooned from a private issue dealt with by individual recording labels into a major political and legal battle. Groups like the Recording Industry Association of America (RIAA) and the International Federation of the Phonographic Industry (IFPI) have launched a full time battle to combat what had been judged blatant theft of songs. The latest statistics blame piracy for a $4.2 billion loss in 2001 [32].

Trying to combat the multi-billion dollar theft of intellectual property is not a simple task. Years of legal and political debate will be needed to establish business regulations and relationships between the United States and foreign countries. Behind the scenes, technologies involving steganographic watermarks and serial numbers are seen as a powerful tool to help even the score. Copyright protection is now driving the emergence of steganography in the commercial sector.

As summarized by Sandy Shaw, University of Edinburgh, there are three main strategies being researched to help protect intellectual property.

> a) *Watermarking*: A technique for embedding hidden data that attaches copyright protection information to a digital object. This provides an indication of ownership of the object, and possibly other information that conveys conditions of use.
>
> b) *Fingerprinting*: A type of watermark that identifies the recipient of a digital object as well as its owner (i.e. a 'serial number' assigned by the vendor to a given purchaser). This is intended to act as a deterrent to illegal redistribution by enabling the owner of the data object to identify the original buyer of the redistributed copy.
>
> c) *Digital signatures*: A mechanism employed in public-key cryptosystems (PKCS) that enables the originator of an information object to generate a signature, by encipherment (using a private key) of a compressed string derived from the object. The digital signature can provide a recipient with proof of the authenticity of the object's originator.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

> The first two of these, watermarking and fingerprinting, are closely related, as aspects of 'data hiding' technology (also known as *steganography*). Digital signatures support origin authentication and content integrity services and belong to the field of *cryptography* [33].

Even though significant progress has been made in testing these watermarks and serial numbers as a proof of concept, little progress has been made to get wide spread adoption in either the software or music recording industries. Beyond the obvious political issues, the biggest challenge to implementing any copyright protection technology is actually finding a solution that is tamper proof. Unfortunately, most attempts at watermarking or fingerprinting media have been found to be less than successful. In as early as 1998, Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn presented to *the Second workshop on information hiding, Portland, OR* [34]. The researchers demonstrated that most of the steganographic processes for watermarking and fingerprinting could be easily disabled or even removed. In conclusion, recommendations were made to help further the development of sufficient copyright protection schemes.

Currently available as freeware, tools like Stirmark, Unzign and 2Mosaic are among some utilities designed to disable or remove the technologies mentioned above [35]. Recent history has shown that like with the Secure Digital Music Initiative's $10,000 challenge[36], as other watermarking technologies emerge, there were always be a strong underground movement ready to test the solutions offered [42].

Uses of Steganography: Malicious Actions and Criminal Protection

While steganography is making gains in popularity as a privacy tool with the federal government and a copyright protection tool with publishing industries, steganography has the most potential as a malicious tool for online criminals.

According to the 2002 Computer Crime and Security Survey, published by the Computer Security Institute with the participation of the FBI, "the findings of the "2002 Computer Crime and Security Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting." [37]. With businesses continually moving to the Internet, the computer underground has continued to look for new and innovative ways to create problems and circumvent corporate security plans.

Besides the standard use of steganography to secretly communicate between entities or to sneak data out of a corporation, steganography has now presented itself as a new vehicle for malware. Steganography's basic premise is the hiding of data, perhaps malicious data, within seemingly normal data. This premise is also the modus operandi of a trojan. Whereas trojans have specifically appeared in the past as part of an executable binary, steganography promises to bring text, graphics, audio and video into the arena.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For example, steganography can be used to deposit dangerous scripts on the machines of unsuspecting users. The cover medium can be as simple as images normally downloaded as part of a web page. Long lost are the days of text based web browsers. The Internet is about instant information, complete with illustrations. Specialty pages that contain desktop themes, wallpapers or MP3 files could be virtual repositories for powerful scripts waiting to be unleashed. Pornography sites would be a target rich environment with graphic and video files that get downloaded in huge batches. Imagine embedding a pair of Perl scripts that act as a sniffer [38] inside of an MP3 file. The audio file gets downloaded and played on a personal computer without the end user hearing any problem with the song. Theoretically, to trigger the contents of the file, a specific webpage with a hostile ActiveX control or Javascript could be designed to extract the embedded Perl scripts and execute them. Simpler yet, a small executable could be mailed masquerading as a security patch for MP3 audio player software. The odds favor a large number of people will execute the code, even though they cannot verify the legitimacy of the source. As is often the case, the security of a resource is at risk as long as people are involved in the solution. Of course, a virus could also be designed to take advantage of steganography. The virus could be of two parts, one containing the trojaned MP3 file containing a destructive payload. The second part would be a lightweight, nimble piece of code that replicates, locates, extracts and executes the infected MP3 source. This concept of a virus using steganographic techniques has been well explored in a white paper entitled, *VIRAL COMPUTER WARFARE VIA ACTIVATION ENGINE EMPLOYING STEGANOGRAPHY* [39], by Captain Dale Lathrop, USAF.

Defense Strategies and Mechanisms

The biggest surprise when researching steganography and its role as a security solution is that almost all security vendors have avoided this technology. The few vendors that do have steganography and steganalysis tools are usually marketed in data forensics, not information security. Frequently these vendors are targeting law enforcement or the federal government as their customer segment. In this next section, this paper will examine why current popular security solutions are not effective for preventing steganography as a covert communications channel or delivery mechanism for malware. An examination of effective strategies and tools will then be presented.

When planning a strategy to defend a corporate network and the information resources within, popular theory involves a defense in depth concept similar to defending a castle with a moat, drawbridge and multiple sets of walls. Many companies mimic this concept with an outside-in approach beginning with firewalls and router filtering. Eventually, companies implement solutions closer and closer to the hosts inside the network concluding with anti-virus software. The exact choice of defense tactics varies greatly from company to company and may or may not include solutions like network and host intrusion detection, proxies, and VPNs. Unfortunately, these products implemented offered by vendors are not steganographic aware.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anti-virus software vendors have been aware of steganographic techniques at least since the late 1990s when various research papers pointed out the tools shortcomings. For this paper, research of three leading anti-virus software packages confirmed that these programs do not scan graphic, audio or video files by default. A simple test of embedding a Perl script inside a jpeg and mp3 file resulted in a clean bill of health by each of the three products. Even by reconfiguring said programs to look at those file extensions provides no further scanning ability for steganographically hidden payloads. See table below.

Function	AV product #1	AV product #2	AV product #3
Scan graphic, audio, video	NO	NO	NO
Steganography aware	NO	NO	NO
Detect Stego type actions	NO	NO	NO
Aware of Stego utils	NO	NO	NO
Mention of Stego in docs or website	YES	NO	NO

An additional review of capabilities on perimeter defense mechanisms like firewalls and network IDS revealed similar weaknesses. The closest solution found in traditional security software was a content filtering product that could catch steganographic tools when they were attachments in downloads or emails. This feature does not catch steganographic content, but merely tries to prevent those types of tools from the hands of end users. This lack of attention in the traditional security marketplace can only be explained by the fact that malware involving steganographic techniques has only been the subject of research papers and not a present threat in the wild. But given the fact that these concepts have already been proved in research, the few forensics focused vendors that do have solutions are going to find themselves in an advantageous position in the near future.

Whatever the explanation, the fact remains that there are few solutions available to the corporate world for the detection of steganographic content in text, graphic, audio or video sources. Marketed directly as a steganalysis tool, Stegdetect [40] and Steg Watch [24] provide the ability to detect steganographic content in various graphic, audio and video media. Stegdetect is offered as a freeware solution while Steg Watch is a commercial product developed in conjunction with the Department of Defense. Additionally, Foundstone offers their Forensic Toolkit [41] that can be used to detect alternate data streams, a technique for manipulating NTFS file systems to hide information.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The only caveat with these tools is that they enable you to detect the presence of hidden information, but as most of the steganography tools make use of encryption, the contents of such information will still remain secret. The greatest challenge to implementing steganalyis solutions is merely the practicality of the act itself. If any document, html, audio, video or graphic file can be a potential harbor for hidden information, then the problem appears to almost insurmountable. Any given corporate website can have tens of thousands of files that would need to be examined. On a given day, a large network might pass an equally large amount of email internally. Even though there has been research done on use automation and web crawlers, for a major ISP, the task of scanning every potential file out there is basically not worth the investment in time.

Conclusion

In conclusion, steganography is still an obscure science in the field of information security, despite a long history of use by governments and military. The fact is that the security industry is not properly educated about or equipped with tools to deal with steganographic content. As the potential for abuse of steganography appears to be limitless, the underground of hackers, crackers and general hooligans will no doubt engineer steganographic enabled malware. Hopefully, as organizations such as SANS continue to educate people to the risks, perhaps some additional focus in the commercial sector will begin. However, as has often been the case, it appears that serious progress will not be made to address the risks, until a loss occurs and someone's misfortune make the headlines.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

[1] steganography- Webopedia
http://www.webopedia.com/TERM/s/steganography.html

[2] Stefan Katzenbeisser, Fabien A.P. Petitcolas, editors. "Information hiding techniques for steganography and digital watermarking", Boston : Artech House, 2000.

[3] Sellars, Duncan. "An Introduction to Steganography".
http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html

[4] How to Make Invisible Ink
http://www.iit.edu/~smile/ch9602.html

[5] Petitcolas, Fabien A. P., "History of Steganography"
http://www.cl.cam.ac.uk/~fapp2/steganography/history.html

[6] Leary, Penn, "The Second Cryptographic Shakespeare"
http://home.att.net/~mleary/

[7] Looking For Shakespeare
http://www.theatlantic.com/unbound/flashbks/shakes/shakint.htm

[8] World War I blackout continues: Invisible ink's invisible secret
http://detnews.com/2001/nation/0106/09/nation-234164.htm

[9] Merriam-Webster Online
http://www.m-w.com/cgi-bin/dictionary

[10] Johnson, Neil F., " Steganography"
http://www.jjtc.com/stegdoc/sec202.html

[11] Bin Laden: Steganography Master?
http://www.wired.com/news/politics/0,1283,41658,00.html

[12] Steganography Software
http://members.tripod.com/steganography/stego/software.html

[13] Steganos GmbH Homepage
http://www.steganos.com/en/index.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[14] Jteg Shell
http://www.tiac.net/users/korejwa/jsteg.htm

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

[16] BMP Secrets: Steganographical Program by Parallel Worlds
http://www.pworlds.com/products/i_secrets.html

[17] S-Tools v4
http://members.tripod.com/steganography/stego/s-tools4.html

[18] wbStego Steganography Tool
http://wbstego.wbailer.com/

[19] mp3Stego
http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/

[19] DataMark
http://www.datamark-tech.com/datamark.html

[20] Texthide – Hiding of any data in text
http://www.compris.com/subitext/

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

[22] Sam's Big Play Maker
http://www.scramdisk.clara.net/play/playmaker.html

[23] Bin Laden exploits technology to suit his needs
http://www.cnn.com/2001/US/09/20/inv.terrorist.search/index.html

[24] Wetstone Technologies – Intrusion Detection, Cyber Forensics, Data Integrity,Secure Timestamping
http://www.wetstonetech.com/prod-stegowatch.htm

[25] NSA, Pentagon, Police Fund Research Into Steganography
http://www.info-sec.com/crypto/01/crypto_022001a_j.shtml

[26] Researcher's grant targets digital security
http://inside.binghamton.edu/May-June/10MAY01/fridrich.html

[27] Intellectual Property Crimes: VIII. Theft of Commercial Trade Secrets
http://www.cybercrime.gov/ipmanual/08ipma.htm#VIII.B.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[28] Computer Crime and Intellectual Property Section (CCIPS)
http://www.cybercrime.gov/eeapub.htm

[29] Economic Espionage Links
http://www.pimall.com/nais/econesp.html

[30] Global Software Piracy Cost $11.8 Billion - Study
http://www.newsbytes.com/news/01/165930.html

[31] FBI Busts Four Alleged Software Pirates
http://www.pcworld.com/news/article/0,aid,57883,00.asp

[32] Piracy in spotlight at annual music sales event
http://www.azcentral.com/news/articles/0415ENTERTAINMENT-MEDIA-MUSIC-SALES-DC.html

[33] Shaw, Sandy, "Overview of Watermarks, Fingerprints, and Digital Signatures"
http://www.jtap.ac.uk/reports/htm/jtap-034.html

[34] Petitcolas, Fabian AP, Anderson, Ross J., Kuhn, Markus G. Kuhn, "Attacks on Copyright Marking Systems", 1998
http://www.cl.cam.ac.uk/users/fapp2/publications/ih98-attacks.pdf

[35] Peticolas, Fabian AP – "Software"
http://www.cl.cam.ac.uk/users/fapp2/software/index.html

[36] SDMI offers $10,000 challenge to hackers
http://news.com.com/2100-1023-245518.html?legacy=cnet

[37] Cyber crime bleeds U.S. corporations, survey shows
http://www.gocsi.com/press/20020407.html

[38] Example Web Packet Sniffer
http://stein.cshl.org/~lstein/talks/WWW6/sniffer/

[39] Lathrop, Dale A, "VIRAL COMPUTER WARFARE VIA ACTIVATION ENGINE EMPLOYING STEGANOGRAPHY"
http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2000/afit-gcs-eng-00m-14.htm

[40] Outguess - Detection
http://www.outguess.org/detection.php

© SANS Institute 2000 - 2002, Author retains full rights.

[41] Foundstone- Free Tools
http://www.foundstone.com/knowledge/forensics.html

[42] SDMI cracked!
http://www.salon.com/tech/log/2000/10/12/sdmi_hacked/

[43] Boni, Williams; Kovacich, Dr. Gerald L, *Netspionage The Global Threat to Information,* Butterworth-Heinemann, MA, 2000, pp104-105

Schneier, Bruce, *Secrets and Lies Digital Security in a Networked World*, John Wiley and Sons, Inc., New York, 2000, pp245-246

© SANS Institute 2000 - 2002, Author retains full rights.