Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 75-80 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

STEGANOGRAPHY AS A MEANS OF ATTACKING INFORMATION SYSTEMS

Anna Romanova [1], Sergiy Toliupa [2]
[1]Taras Shevchenko University of Kyiv, Faculty of Information Technology, [2] Taras Shevchenko University of Kyiv, Faculty of Information Technology

ABSTRACT. An analysis of steganography methods that are can be potentially used as instruments in attacks on information and communication systems is presented. The possible solutions to ensure resilience to such attacks are presented.

Keywords: steganography, TEMPEST, covert channel, information protection

Cryptography is widely used as one of the most efficient and approbated methods of critical information resources protection. Nevertheless, in particular cases it might be more effective to hide the communication channel itself instead of making the information within it unreadable. Such a practice, namely concealing data within unsuspicious, innocent-looking containers, is called steganography.

Any concept might have a double application. While being primarily considered a means of information protection, steganography can be used with ill intentions, as well. In fact, several high-tech attacks are based on the hidden data transmission, and contemporary methods of counteraction do not provide satisfactory level of resilience to those. These attacks are not always considered to be steganography-based, as they, for the most part, use a variety of features, characteristic for information and communication systems – physical effects, transmission protocols, communication infrastructure, specific features of software, cryptography etc. Nevertheless, the attack requires a classical statement of the task of steganography – how to transmit data so that a potential attacker could not acquire them due to not knowing about the presence of a transmission channel, even if he or she has a suspicion about one and the possible methods are known. In this case, though, an attacker and a legitimate user switch places, and the counteraction involves mainly the preservation of information resources.

In such attacks, the main advantage of steganography becomes the main source of threat – the channels of the attack, not to mention the information about the attacker left in the channels, cannot be identified due to the nature of the method. In other words, attacks become invisible, as does the transmission channel. The fact of trespassing itself cannot be easily detected or proven.

The purpose of this article is to conduct an analysis of attacks that are carried out with the use of steganography methods as their basis, and are directed against information and communication systems. Both existing and potential methods are presented.

1. Steganography as a means of hiding information

1.1. Basic terminology

Steganography is an art and science of storing and transferring secret messages within covert channels that are based on and created inside open channels in such a way that the cover data is perceived as if not having any embedded messages for its unplanned recipients.

The main concepts are:

- Container b (also: carrier) is open data used to conceal secret information;
- Message m (also: payload) is secret information to be concealed;

- Key k is secret information that is known only to a legitimate user and defines a specific concealment algorithm;
- Empty container c (also: unmodified container) is a container devoid of any secret data; it is a sequence of lc-long elements;
- Modified container s (also: package, steganogramme) is the one that contains a secret message;
- Steganographic algorithm means two transforms, a direct F: M x B x K → B and an inverse one F-1: B x K → M;
- Steganographic system (also: steganosystem) is a totality of messages, secret keys, containers and transforms that connect them [1, 3].

Most steganography methods are based on two key principles:

- Human senses cannot distinguish slight changes in colour, shape and sound perception;
- Consequently, there are files that do not demand absolute preciseness and therefore can be modified without losing their functional value.

As a result, said methods imply allocation of insignificant fragments of the container and replacement of the information within them with information that needs to be hidden.

Finally, the process of encoded steganogramme detection is called *steganoanalysis*.

Mostly, steganography uses the data concealment within digital images and audio files, less so video files and text. Electronic communications may also include hiding data inside of a transport layer (program or protocol) [4].

Starting with non-digital methods, physical steganography technics cannot be omitted. They have been developing for centuries and include, for example, blinking one's eyes in Morse code to spell a secret message [5].

Another example is adding tiny yellow dots to each page while printing a document. They are not detectable by the bare eye and contain the model, serial number and timestamps. This information cannot be obtained from a computer file and is embedded in a printout using dot-matrix code. The technology is used by many brand color laser printers, such as Xerox and Hewlett-Packard for traceability reasons [6].

The most popular methods of embedding data within an image container include Least Significant Bit method (LSB) (Sequential Insertion), LSB Psuedo Random Insertion, Palette permutation, Relative DCT (Discrete Cosine Transform) values change method, Fridrich method, Spread-Spectrum methods, and embedding pictures within video-files [2, 3, 5].

Audio steganography uses LSB-method for audio-files, Phase coding method, and echo-signal use [3, 7]:

Linguistic steganography [3]:

- Random interval methods. Changing the number of spaces in the end of the text string does not cause significant changes in the meaning of the sentence. What is more, an average reader is unlikely to detect insignificant space modifications:
  - Changing the interval between sentences. One or two additional spaces are added after the sentence.
  - Changing the number of spaces in the end of text lines. Spaces are added according to the secret bit to be hidden. Two spaces encode one bit a line, four spaces – two bits etcetera.
  - Changing the number of spaces between words in a flattened text. When the text is width aligned, spaces between words are not of the same length and some of them can be used to hide data.

- Making the text of the same colour as the background [5];
- Using similarly looking Unicode and ASCII characters [4, 8];
- Using non-printable Unicode characters [8];
- Creating a pattern of deliberate errors and/or marked corrections [4].

Some other methods:

- Converting a file so that it has the statistical characteristics of another one [4];
- Format steganography;
- Blog-steganography. Secret data is added as commentary pin boards on social networks [5].

Surely, the list above is not at all exhaustive. New methods and applications are being continuously developed, effectively putting steganography at top positions within the field of security.

2. Steganography methods used as instruments for attacks

To identify the methods of steganography that can be used as tools for attacks, it is necessary to first determine channels of information transmission that can be used in a covert way. Those are numerous, and file formatting, as well as different emanations from electronic devices are among them.

2.1. Format steganography

Perhaps, the easiest and the most well-known way, which is actually a steganography method, is using legitimate features of file formats to carry hidden malicious software within their structure. A file of every format contains specific fields, which ensure that the former will be processed correctly on the target computer. Some of these fields are optional, or more strictly – information that they contain is not vital for the file. Thus, changing data bits in these fields most probably will not lead to errors while operating with the file. Such characteristics make these formats perfect containers [10].

A vivid example is a virus Win95.CIH – specific malware which is embedded in *.exe files by using Portable Executable format features. This format includes a lot of additional data which are grouped according to their functions. Every group gets its own section in the file structure, and the size of the sections is predefined. If they are not entirely filled with data, it means the file contains a lot of spare space. For example, the first section is only for the PE header, so a big part of the virus uses it as a covert container [11].

This method is no commonly seen as a steganography method, though the analysis of scientific works has shown that such a question has not been even risen. A covert channel is being used, and data are being secretly embedded into the containers, which makes this a classical steganographic system. The next step in this research is to provide a mathematical model for a steganosystem used in a potential attack with file formats as carriers of malicious software and other instruments of intrusion and destruction.

2.2. Soft Tempest

In fact, there are a lot of ways to covertly transmit necessary information to the target system. Not only harmless files but also network protocols can be used as efficient containers within the attacker’s steganography system. Nevertheless, necessary means depend on the final objective of the attack. If the goal is to steal data, there is need for both an inward and an outward information flow. Getting information into a system is important. A more interesting question, though, is how to get the stolen data out without raising suspicion of a legitimate user.

While operating, every electronic device (including those inside a computer) gives off compromising emanations – electromagnetic emanations, which can be demodulated and accordingly processed to illegitimately get the critical information from them. These are called TEMPEST emanations after an American standard on the matter.

Contemporary TEMPEST-based attacks tend to become more and more sophisticated as the countermeasures are being continuously enhanced, as well. Systems are contaminated with the malicious software which then conducts the search of necessary information (key data, passwords, specific files etc) and induces the leak through TEMPEST emanation. For example, if reception of the signal is the one from the monitor, then the information will be, say, amplitude modulated and sent as a visual picture to the monitor. The obvious disadvantage is that such an activity cannot be missed by an operator and will be deemed highly suspicious, which, on its part, will lead to finding and neutralizing the virus.

M. Kuhn and R. Anderson conducted a series of experiment in which they shown a possible solution [12]. The human eye is more sensitive to low-frequency than to high-frequency vibrations, while TEMPEST receivers work vice versa. What is more, any devices primarily perceive luminosity in a linear way, while humans are more sensitive for the dark colours. This difference in sensitivity perception can be used to embed a message in the emanation and make it invisible to an unsuspecting user. The suggested method is to control and modify monitor dithering patterns. Pixels of two colours put in a check pattern are seen as a uniform colour, on the one side; on the other side, they create a high-frequency signal, which is best received by TEMPEST equipment with the following use of gamma-correction. Basically, the target computer is programmed so that it acts as a radio transmitter and emits a compound TEMPEST signal: a legitimate user observes one picture, and the attacker receives another – embedded – one on the monitor of his/her TEMPEST receiver.

The only suggested method of counteraction, which is specific enough for this very type of attack, is still based on using the difference in perception sensitivity between humans and devices. TEMPEST fonts are designed with top 30% of the Fourier transform of the signal removed, which is most probably not noticed by a human eye, but makes it impossible to receive a strong TEMPEST signal [12]. Nevertheless, special equipment with necessary parameters (enhanced sensitivity to low-frequency emanations) might be designed, which will make the use of such fonts ineffective.

2.3. Acoustic emanations as containers

Electromagnetic fields are not the only by-product of the computer systems operation. A. Shamir and E. Tromer published the results of their research, in which they showed that computer emit high-pitched noise while operation, due to vibration in some of their electronic components [13].

A series of experiments conducted by the scientist revealed that acoustic emanations can provide a potential attacker with information about what kind of software is currently running on the target system, as well as leak data on security-related parameters and computations. For example, loops of CPU instructions were highly distinguishable, and different RSA keys appeared to induce different sound patterns. To extract individual keys, the technic of acoustic cryptoanalysis was presented (applicable to GnuPG's implementation of RSA). According to the results, it takes about an hour to extract full keys from a target computer, irrespectively to their models and manufacturers. The key piece of equipment used for the attack is a microphone, and that of a mobile phone was demonstrated to be enough. Apart form acoustics, the scientists demonstrated a low-bandwidth attack, based on the same principles. The

main difference was that the attacker had to get the leakage from ends of VGA, Ethernet, USB or other cables [13].

If electromagnetic emanations can be used as containers in steganography systems, acoustic waves can be, too. The first case could be based on the nature of sound perception itself – the classical steganography technic. Human hearing systems cannot distinguish slight variations in an acoustic flow. Here, any known method, mentioned above (Least Significant Bit, Echo-signal use etc) can be used to embed stolen information in parasitic sounds, emitted by the target computer. The second possible scenario is similar to the use of emanations in Soft Tempest. Sound dithering is a widely used method in music digital processing. The principle is the following: any piece of musical record might contain extensive frequency transitions that are too slow and smooth. This is where so called quantization noise can appear. If the level of frequency fluctuation is insignificant, the processing software simplifies the sound by removing the frequencies that exceed some medium limit. To cope with such a situation, special noises are generated and gradually added to the record. In music processing, this technic allows to achieve a natural sound lost during quantization.

It is possible to suggest, that the same technic can be used in attacking steganography systems. The noise emitted by a computer is quite stable. It is not foiled by fan system noise, as critical acoustic signals appear to be mostly above 10 KHz, while a typical fan noise along with other noises lie in a much lower frequency band [13]. Task-switching is not a problem either, as it is the tasks that carry distinguishable acoustic spectral signatures. The same can be said about several computers working simultaneously in a closed space: they can be told apart using different sound patterns, as their depend on specific hardware, temperatures inside and outside the system, humidity, and other conditions. Thus, it acoustic emanations seem to be a sufficient container, while dithering can be accordingly modified and applied as an embedment method.

The only suitable countermeasure seems to be the use of sound dampening equipment that can diminish the level of high-frequency leakage. As for means of active protection, strong wide-band noise source can serve for masking the critical data signals. Rough-scale behaving algorithms are another solution: despite somewhat diminishing the level of performance, they can thwart side-channel attacks by shuffling the signal and making it thus useless for the attacker [13]. In addition, electronic components of the system should be those of the highest quality, designed to reduce the level of acoustic and any other leakage.

Nevertheless, at this point, efficiency of such protection methods is rather relevant, as sound-proving degrades other performance features along with being quite expensive. At the same time, due to the need of ventilation, there are still open parts in the cases, so their structure has to be constructed to shuffle outcoming noises very efficiently.

3. Conclusion

Stenganography is a powerful means of information protection. Nevertheless, it has to be also regarded as an instrument for a potential attacker, with all of the advantages turned threats.

Compromising emanations of different physical nature are invisible and can only be noticed with the use of special equipment. Using steganography technics for the attacks ensures that the fact of using those emanations is efficiently hidden, and the system operations remains unsuspicious. This is exactly why there is need to consider technics described above a real threat for information and communication

systems, and to join academic and technical potential to develop cost-effective and technically efficient counteracting means.

REFERENCES

[1] Зорин Е.Е., Чичварин Н.В.: Стеганография в САПР. Учебное пособие. МГТУ им. Н.Э. Баумана, Москва (pdf).

[2] Alexandre Miguel Ferreira: An Overview on Hiding and Detecting Stego-data in Video Streams. University of Amsterdam, System & Network Engineering – Research Project II, March 23 2015.

[3] Konakhovich G. F., Puzyrenko A. Yu.: Computer steganography. Theory and practice with Mathcad (Rus). MK-Press Kyiv, Ukraine 2006.

[4] Fridrich, jessica, M. Goljan, D. Soukal: Searching for the Stego Key. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI 2004 (pdf): http://www.ws.binghamton.edu/fridrich/Research/Keysearch_SPIE.pdf.

[5] Christopher League: An overview of digital steganography, particularly within images, for the computationally curious. Long Island University 2015: https://www.youtube.com/watch?v=-7FBPgQDX5o.

[6] Secret Code in Color Printers Lets Government Track You; Tiny Dots Show Where and When You Made Your Print. Electronic Frontier Foundation October 2005: https://www.eff.org/press/archives/2005/10/16.

[7] Echo Data Hiding (html): http://www.slidefinder.net/a/audio_steganography_echo_data_hiding/24367218.

[8] Akbas E. Ali: A New Text Steganography Method by Using Non-Printing Unicode Characters. Eng& Tech. Journal, 28 (1) 2010 (pdf): http://www.uotechnology.edu.iq/tec_magaz/volume282010/No.1.2010/researches/Text%287%29.pdf.

[9] Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А.: Стеганография, цифровые водяные знаки и стеганоанализ. Москва: Вузовская книга 2009.

[10] Anna Romanova, Sergiy Toliupa: Perspective steganographic solutions and their application. Proceedings of the VII Inter University Conference „Engineer of XXI Century" at the University of Bielsko-Biala (ATH), December 08, 2017, Bielsko-Biala, Poland. Volume 2 – p 269-278.

[11] С. Чеховский: Современные методы скрытой передачи информации путем программного управления излучением компьютеры. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, випуск 7, 2003.

[12] M.G. Kuhn, R. Anderson: Soft Tempest: Hidden data transmission using electromagnetic emanations. University of Cambridge, Computer Laboratory, New Museum Site, 1998 (pdf): https://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf.

[13] D. Genkin, A. Shamir, E. Tromer: RSA key extraction via low-bandwidth acoustic cryptoanalysis.Tel Aviv University, December 18, 2013 (pdf): http://www.cs.tau.ac.il/~tromer/papers/acoustic-20131218.pdf.