Cybersecurity and National Defence

—

Steganography: steganalysis

Alberto Eusebio, Francesco Imparato, Federico Morro,
Salvatore Orlando, Giulia Rivetti

Abstract

Contents

1 Introduction

Steganography is the technique of hiding a message inside another message or a physical object.[1] The word *steganography* comes from the Greek word *steganographia*, which is the combination of *steganós* meaning "covered" and *-graphia* meaning "writing".

The first testimonials of the use of steganography date back to 440 BC in Greece mentioned by Herodotus in his *Histories*: Histitateus sent a message to Aristagoras by writing a text message on the shaved head of one of his servants and then waited till the hair of the servant had regrow to sent him to Aristagoras. Moreover steganography has been used for centuries in different ways such as secret inks, morse code hidden inside physical objects or encoded in eyes blinking (Jeremiah Denton, tortured prisoner-of-war in 1966 during the korean war, encoded in this way an help message during a TV report) or microdots embedded in paper or in clothes used by espionage agents during and after the World War II.

In digital steganography a message or a file is concealed within another file; in particular, electronic communications may contain a steganographic coding inside a information vehicle such as a document, a program or a media file (image, audio or video). Media files are ideal for hiding messages since due to their large size, the modification needed to encode a steganographic coding cause a subtle change that is unlikely to notice for someone who is not looking for it. This is one of the greatest differences of steganography with respect to cryptography: in cryptography the encrypted messages are visible so they attract interest and it's more likely that they will be subject to some type of attacks to be decoded.

In this paper we will focus on steganalysis, the study of detecting and, if possible, recovering hidden messages encoded using steganography, the way in which it can be performed, examples of its application in known cases and the threats and opportunities regarding the cybersecurity implications of its use in digital and communications systems.

We can call steganalysis successful (and consequentially that the steganography is broken) when there is the evidence of an hidden message in the cover signal. Moreover, the embedded information can also be crypted, in that case the attacker (the one who tries to find the hidden message) will have to perform cryptanalysis in order to decrypt the information.

2 Steganography

As we already stated, steganography is used to hide a message in a *cover type*. We can define a cover type as the mean used to communicate, which can be a text file, an image, an audio recording, but also people, like in the case of the servants that we have mentioned earlier, etc...

In all these cases, the message has been *embedded* into the cover type. Here we can make a distinction between steganography and watermarking since in both cases a message is encoded into a communication's mean, but with different purposes.

2.1 Steganography

2.2 Watermarking

3 Steganalysis

Steganalysis is the branch os study dedicated at analysing the methods and the vectors used to transmit an hidden message in order to retrieve such message whenever it is present. Unlike chryptanalysis where the message may even be apparent but enchrypted, in steganalysis the study of the message starts from a suspect.

3.1 Methods

Hereinafter we will present the two type of methods used in steganalysis in order to obtain the secret message

3.1.1 Statistical

3.1.2 Structural

3.2 Images

3.3 Audio

3.4 Text

3.5 TCP/IP

3.5.1 Introduction

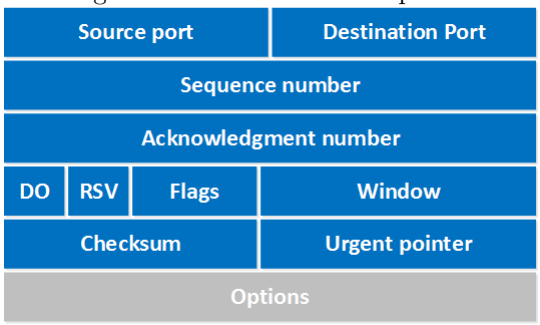
Before treating such topic we must briefly discuss the behaviour of the TCP/IP (**Internet protocol suit**) communications.

IP (Internet Protocol) is at the basis of internet communication. The protocol exploits the principle of encapsulation, sending packets composed by a *header* which contains information such as the **destination address** and **source address** and a *payload* which represents the actual data to be transmitted. Since physical channels usually have a limited MTU[1], then the data is usually fragmented in smaller chunks, wrapped into an header and only then transmitted.

TCP (Transmission Control protocol) is a protocol used for reliable(little information loss), ordered, error-checked data transmission between a machine hosting the data (**Server**) and another requiring such data (**Client**). It is performed previous a three-way handshake which estabilishes a connection between server and client, thus preparing a reliable communication channel.

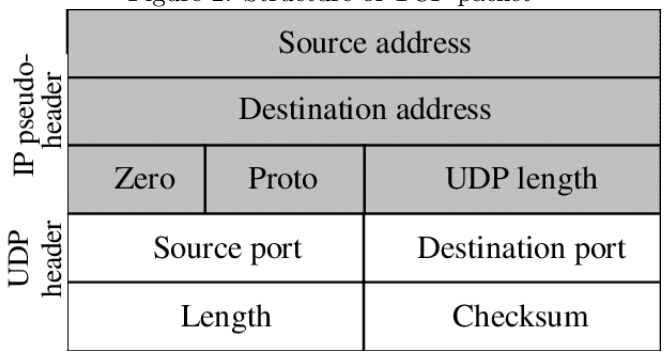
UDP (User Datagram Protocol), contrary to TCP, is less reliable but faster. It broadcasts the data in an unordered and uncontrolled way to the receiver. There is no need to estabilishing a connection in order to implement such protocol.

Figure 1: Structure of TCP packet



[1] Maximum Transmission Unit

Figure 2: Structure of TCP packet



3.5.2 Exploits and protection tools

As you could notice from the previous figures, the first part of the header is the same. This is because it is part of the IP protocol itself. In the second part of each header we find different types of metadata which are specific for each protocol. Generally the metadat contained in the header is redundant for the transmission of the message itself and this redundancy may become a target for a *stego-algorithm*[2] which starting from a *cover-network packet sequence*[3] and a *covert message*, can generate a sequence of packets(each one embedding a portion of the covered message) which will be sent over the network.

This procedure is not a *risk-free* approach for the attacker who wishes to send the *cover-network packet sequence*, since it is possible that the data will be currupted during transmission or there could be losses using non-reliable transport protocols(UDP). Other criticalities of such method stay in the fact that the sequence of packets will most likely traverse multiple nodes in the network before reaching the target, and the message may be detected by these nodes.

The defense against Steganography in TCP/IP communication consists in a series of standards which are implemented by the devices on the internet and that we will illustrate through some examples.

Tof(Type of service) bits are a field in the TCP header which are nowdays rarely used. This could open doors to a steganographic attack if modern operating systems did not set them to zero by default. A warden monitoring the channel could immediately signal an error.

IP ID is a field in the Internet Protocol which is used to assist the receiver in reassemblying the fragmented packets. This field consist of randomly unique numbers representing a packet. It is possible to insert other types of information in this field by simply conform to the uniqueness constraint. Since in many cases the numbers used for the IP ID are not random, by knowing the charachteristics of the sender it is possible to detect an infiltration.

IP Fragment Offset is an offset which is present in the IP header which helps the receiver to reconstruct the sequence of bits from the fragmented sequence. Modulating the size of the fragments changes the offset field in the header and thus a message could be sent. The protection against this method is simply checking the size of the packets relative to the MTU and so even in this case a warden can easily detect an error.

TCP sequence number is a field in the TCP header which stores the randomly chosen position(for security reasons) of the first byte to be transmitted through the channel. The steganographic method consists in replacing this field with the data to be sent. Being random it is more difficult to spot a breach in the channel. In this case the usage of a SVM[4], a machine learning tool able to identify patterns inside the data transmitted could come into hand. However an error could be detected even simply by checking the presence of repetitions in the stream(not admitted by design).

[2] an algorithm used for steganography
[3] a sequence of packets which will be transmitted over the network acting as a cover for the hidden messace
[4] Support Vector Machine

Timestamp modulation is another technique of steganography which operate by modifing the LSB[5] of the timestamp of a TCP packet in order to represent a '1'. The covert message is thus embedded into the data stream. Since the TCP Timestamp support is not universal, machines not supporting such feature may detect the hidden message.

[5]Least Significant bit

References

[1] Merriam Webster. *Steganography definition*. URL: https://www.merriam-webster.com/dictionary/steganography.