Steganographic Attack Methodologies

Gaurav Saini
Dept. of Information Technology
National Institute of Technology
Kurukshetra, 136119
gaurav_11610325@nitkkr.ac.in

Chakrapani Gautam
Dept. of Information Technology
National Institute of Technology
Kurukshetra, 136119
chakrapani_11610577@nitkkr.ac.in

Kalpit Manglunia
Dept. of Information Technology
National Institute of Technology
Kurukshetra, 136119
kalpit_11610343@nitkkr.ac.in

***Abstract*—Steganography is an art of hiding information in various types of files, including digital images, audio, and video through obscurity, or in such a way that it becomes hard to detect it. This paper introduces a cyber-attack approach in which a payload is embedded in the media using steganographic techniques. The target will be a victim running an application that behaves flawlessly for an ordinary digital media, say an image. However, when the image containing the payload gets loaded, the malicious code in it executes and exploits the system.**

I. Introduction

The word ”Steganography” is derived from Greek ”Steganos” meaning hidden or concealed. Thus, ”Steganography” stands for ”concealed writing”. Steganography is a way of hiding of a message within another so that the presence of the hidden message is indiscernible. Steganography uses a medium like an image, video, audio or text file to hide the information inside it in such a way that it is not detectable to the casual eye. The media with hidden information is called stego-media and the media without hidden information is called cover media.

There is a difference between cryptography and steganography. The word ”cryptography” stands for ”secret writing”, whereas ”steganography” stands for ”concealed writing”. Cryptography alters the standard secret message structure through encryption, which can be decrypted through a proper key. On the other hand, the steganography does not employ changes in the structure of the message but conceal the message inside another media file.

II. Motivation

In the present day major havoc is caused over the internet. Steganographic attack is another method to cause such damage. It is one of the most used attack at present but still no proper security measures are present to detect and prevent it.
Another reason is that, steganographic techniques are used in a lot of 'capture the flag' and such events.
So, the main motive of this project is to study the methodologies by which such steganography and steganographic attacks can take place to understand them better and if found, suggest some prevention measures to stop these attacks.

III. History

Several incidents had been observed in past where steganography was used for secret communication. The earliest recorded use of this word dates back to 440 BC when Histiaeus; the Persian Chief Miletus; shaved the head of one of his servants and tattooed a secret message the servants scalp. The message got covered, when the servant grew his hair back. And Histiaeus sent the man to Aristagoras who shaved the mans head and read the secret message.
And also when Demaratus fooled the Persian spies by covering the engraved wooden tablets with wax to secretly forewarn Greece of the arrival of Xerxess naval fleet.

IV. Various Steganography Techniques

There are various types of steganography methods and techniques which are used for embedding a file inside a cover or carrier media.

A. Text Steganography

It is a way of hiding a secret message in a text file by altering the text formatting or altering the characteristics of textual elements. The goal in the design of the decoding techniques is to minimize the visible changes and maximize the reliable decoding.

B. Image Steganography

It is a way of hiding a secret message inside an image by manipulating some of its pixels. The pixel modification is done in such a way that the changes are not visible or, indiscernible. The simple approach of embedding information in the cover image is embedding the bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence. Pixel modification does not results noticible change in the cover image.The secret message is embedded into a carrier image as a noise because human eyes can not detect a difference between the original image and stego image.

C. Audio Steganography

It is a way of hiding the secret messages into digital audio. The human ear can pick up the vibration of the membrane between the frequency range 20Hz to 20kHz. One way to achieve audio steganography is to use Infrasound or/and Ultrasound range to transmit the secret messages.

V. Attacks using steganography

Steganography techniques are widely used in cyber-attacks or crimes. There are various types of threats like ransomware (eg. Cerber, TeslaCrypt) or exploit-kits (Stego/Astrum, DNSChanger, and Sundown) use some form of information hiding techniques.

A. Malware in digital media

The most common way of hiding data is to use digital images as a secret carrier.
Following are the ways used to exploit digital images:-

1) conceal malware settings or a configuration file.
2) embed an URL to download the malicious file.
3) conceal the complete malicious code.

In 2015, Vawtrak/Neverquest malware started utilizing steganography to hide settings in favicons, i.e., innocent-looking pictures widely available in websites. The malware extracts the least significant bits from each images pixel in order to reconstruct a previously embedded URL for downloading its configuration file.

REFERENCES

[1] https://www.clear.rice.edu/elec301/Projects01/steganosaurus/background.html
[2] https://ieeexplore.ieee.org/document/6482411
[3] https://pdfs.semanticscholar.org/2331/1184a7b078945f519e8bf89c719fed7b1f81.pdf
[4] https://arxiv.org/pdf/1401.5561.pdf
[5] https://www.ijraset.com/fileserve.php?FID=8366