Introduction to Steganography

Ms. Rashmi Janbandhu
Lecturer, Information Technology
Rajiv Gandhi College of Engineering & Research
Nagpur, India
rashmi.janbandhu@gmail.com

Mr. Viplove Karhade
Scholar, Computer Science and Engineering
North Eastern University, Boston
viplovekarhade@gmail.com

***Abstract*—**Security is a big issue in today's world. The world today has completely or mostly started working on computers. Computer stores data which can be vital information in the form of electronic files. Providing security to these files is essential. Study was done on various attacks on these files in order to provides a brief introduction of breaches and security holes. The paper consists of background to future perspective of lacunas in security as threats to security are in its evolutionary phase.

Keywords-*Security, computer network, stegnography.*

*****

I. Introduction

The threat to security instigated at the very early stages of computers. The computers were first connected in around 1969, known as Arpanet. This Arpanet was formed by the department of Defense, United States. The electronic files were sent along this network. The files interchanged were of importance and hence needed safe transfer. Thus, the evolution of computer network urged to computer network security.

The whole world uses network as a prime source of communication. The use of network increased decade after decade. The usage of network inspired many developers to work on network and its architecture to make it more security. The complex network architecture became prone to breaches.

Another aspect of security is in the context of intellectual property. The illegal use of data in electronic file is big issue these days and hence security means such as digital certificates, digital signatures etc. are employed.

The paper organization comprises of history of security in network, Steganography.

II. Computer Network security

The computer network security basically comprises of security provided to both the computer and the network in between computers. The data should be secure while stored in computers and also while getting transmitted via networks. Various methods have been discovered to provide safety to the data.

The history of network security shows a significant gap between the technologies associated with security and network. The statement can be proved with the evident presence of International Standardization of Organization's Open System Interconnection model. This model was developed with a thought of making ideal network model. The model has well defined architecture. It has seven layers with well-defined functions. Each layer is independent of the other. This indirectly means that if the functionality of a layer is improved or changed according to need in future then the other layers will not be affected. It also had good and well developed form of protocols required for networking. But although the model was perfect in terms of networking, it did not address any problems of security. Due to the above reason the statement of gap between technologies gets proven.

To bridge this gap between technologies i.e to provide network security, just providing security to the computer won't work. For example let us assume in a network we just provide security to the computers , the result would be the data would be safe within computers but as soon as the data enters the network link the safety is tampered, it is possible that the data would be modified before it reaches its actual destination. The above scenario proves the necessity of security on links also.

A. Features

The computer security has five main pillars to be accomplished in order to provide safety:

- Only the authorized person is allowed to send the data over the network between two computers.
- The data that is getting transferred will not be made public on entering the network link; the data will be private to the sender computer and receiver computer.(after receiving)
- Ensuring the identification of each computer host to the one it is announcing to be.
- The data should be protected as a whole; its alteration or modification has to be protected while getting transmitted via network.
- Preventing backing off after sending data or using the network.

A technique known as Steganography is a well-defined for providing security on network.

III. STEGANOGRAPHY

A. Introduction

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret,

it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

B. Steganography definition and history

Steganography is the skill and knowledge of hidden invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”[1,7].

The thought and practice of hiding information has a long history. In Histories the Greek noble men if wanted to communicate with his son in law somewhere far they used to shave the head of one of their trusted man. Once shaved the message was tattod on the head’s skin and then the messenger (trusted man) would let his hair grow again. Once the hair grew to cover the message completely the messenger would depart to the son in law. The son in law would in turn shave the head of the messenger again to retrieve the message again.

C. Steganography in Today’s world

Today the world has mostly or completely shifted to computers for communicating. Thus now electric files are the means of communication and these files will now be the container of secrete messages. The standard and concept of “What You See Is What You Get (WYSIWYG)” which we used for images has got no longer potential to con the steganographer. Images in the computer based format are very potential container of secrete messages, the images can now contain of about thousands of words in it[2].

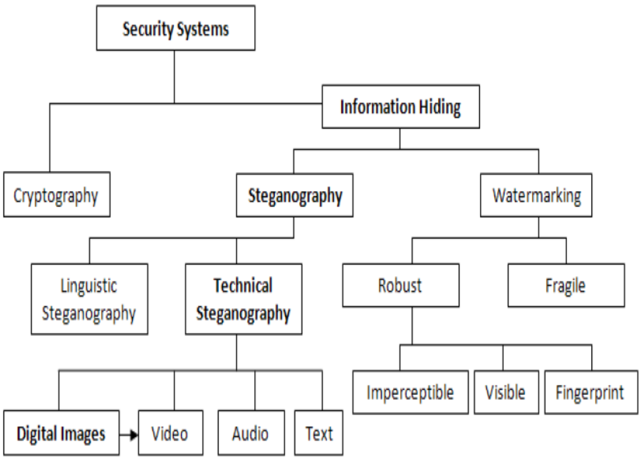

Figure 1. The different embodiment disciplines of information hiding

Steganography researchers have now developed techniques to hide data in digital formats. The popular data formats used are:

- .bmp
- .doc
- .gif
- .jpeg
- .mp3
- .txt
- .wav

These formats were purposely used by researchers because these entire file formats are used widely for communication over the internet in today’s digital world.

IV. STEGANOGRAPHY AND ITS IMPORTANCE

Steganography is a science of covered writing. In initial days steganography was done on papers that were used to convey messages from sender to receiver. One such form of stegnography was use of acidic invisible ink. This ink would be invisible on page. The message written by this ink could only be read if the paper on which it is written is kept in a particular angle in light. The secrete message was first written with the invisible ink and then to make the letter more convincing some message in the format of simple letter was written on the same page. So this was steganography in its initial phase. [3]

Steganography effectively hides the message but does not hide the phenomena that two parties are communicating. The stegnography is a method to hide the secrete data or information in a normal data or information. The normal message used to hide the secrete data is known as carrier. The secret message is embedded in the carrier to form the steganography medium. The stegnographic key is used to hide or encrypt the message. This key will known only to the sender and receiver.

When a image is used to hide a data then after the secretdata is stuffed in the image the resulting image is known as stego-image. Similarly when a data is hidden in the video, the video containing the hidden data is known as stego-video. The process may be summarized as follows:

steganography_medium= hidden_message(information) + carrier(cover-medium) + steganography_key

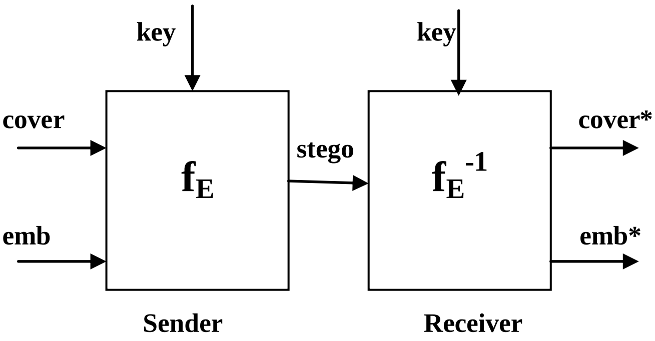

Figure 2. Basics of modern Steganography

Where,

f_E: steganographic function “embedding”

f_E^{-1}: steganographic function “extracting”

cover: cover data in which emb will be hidden

emb: message to be hidden

key: parameter of fE

stego: cover data with the hidden message.

In a digital world, Steganography and Cryptography are both wished-for protecting information from unnecessary parties. Both Steganography and Cryptography are good to protect data but neither technology alone is perfect and both can be conked out. It is for this reason that most experts would suggest using both so as to add more layers of security.

Steganographic technologies are a very vital part of the probable Internet security and confidentiality on open systems such as the Internet. Steganographic researches are basically aiming to compliment the cryptography and bridge the breaches or gaps or security holes in cryptography. The steganography focuses to provide complete security. The researchers have concluded with their studies that most of the governments have put limitations on the methods and complexity of the encryption. With these limitations the methods developed by the developers are relatively weak. These weak logics form the security holes which if attacked can reveal the hidden information very easily. Thus the stegnography is a solution to cover up the security holes and hence stegnography is constantly under evolutions with cryptography.

Steganography is used to hide data inside another data. The sender and receiver both have the knowledge that the secret data is hidden in the message. To add multiple layers of security and to help subside the "crypto versus law" problems previously mentioned, it is a good solution to use steganography in compliment with the cryptographic techniques. Both the methods i.e cryptographic methods and steganographic methods are having pit-falls but both when used together can find solutions to each other’s lacunas. Thus in short we may say that it is beneficial to use a combination of the two methods[4].

V. Classification of Steganography techniques

Steganography is broadly divided into two groups technical and linguistic. Technical steganography uses scientific techniques to hide a message, such as the use of invisible ink or microdots and other size-reduction methods. Linguistic steganography hides the message in the carrier in some nonobvious customs and is further categorized as semagrams or open codes. Below is a graphical representation divisions and their definitions.

The **Semagrams** hides the information using the symbols. These symbols can be very natural looking and may be of day to day use. The semagrams use the layout to hide the data. The positions of the content is used to hide the secrete message of information.

Semagrams can use a sudden changes in text fonts , their sizes, spacing etc to hide the secrete data under a normal looking layout.

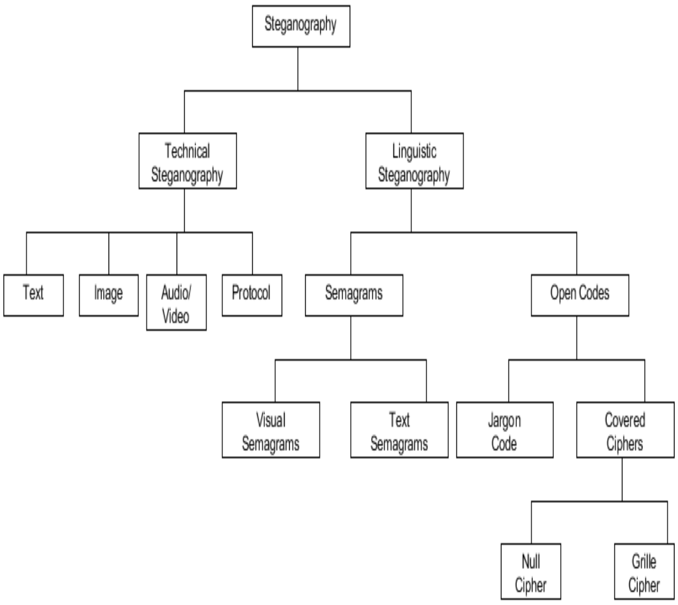

Figure 3. Classification of Steganography

Open codes is hiding the message behind a normal text message. The secrete message is hidden in such a format that the third party other than the sender and receiver won’t be able to retrieve the message. The normal text message used to hide the secrete information is called overt communication message.

Jargon code, is a mechanism in which the sender and receiver create their own language. The language is created using a Specific set of symbols designed by the community using this language. The message written in this language will be meaningless to all others.

Covered or concealment ciphers , is a technique in which the secrete message is encrypted in a normal text with simple logic, which is made known to almost anyone authorized to read the message.

Null Ciphers A null cipher is a logic which is set of rules known prior to encryption and decryption. Example can be: read 1st alphabet of the text:

- WELL ELLEY, NO ENEMY EVER DEEDFULLY TRY OF MAKING EFFECTIVE ENDEVOURS TO. THIS HIGH INTENTIONAL SPEED

MAYOR OF NATIONAL TRETIES HAWARD

Hidden message (reading the first letter of each word) =
WE NEED TO MEET THIS MONTH

There are different kinds of technical steganography like text, image, audio, video, protocol etc. Almost all digital file formats can be used for steganography, but formats with high degree of redundancy are suitable. Redundancy here can be defined as the information which is repeatedly present in the data, and the data could have been easily understood without these repeated content. The redundant bits are the bits which when altered are not detected easily [5]. Image and audio files are widely used for steganography but this doesn't mean that other file formats cannot be used.

Historically, hiding data into text was the significant technique for steganography i.e. hiding secret note in every nth letter of every word of a text message. But since the beginning of the digital era, Text, Images, Audio/video, Protocol, Internet and all the different digital file formats has diminished its importance. Text steganography using digital files is not used frequently because the text does not have much redundant data. The image is consisting of many pixels which are represented as bits. Most of these bits are found as redundantly. And this feature makes the images a vital format for steganography.

Similar method is used to hide secrete data in audio files as that of used for image files. Masking is one of the unique technique which hides the data in audio file in such away which is undetectable to human ears. A light fine audio becomes unperceivable in front of louder audio. This feature creates a space where we can hide the information. Although the above mentioned technique is as good as image steganography but the increase in size of stego-audio give a hint to intruder about the hidden data[6].

VI. Conclusion

The paper provides a brief introduction on what Computer network security consist of. It also addresses idea of the Steganography as a tool for security.

Acknowledgment

The paper contains all the knowledgeable content best known to the authors.

References

[1] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf .

[2] J.C. Judge, Steganography: Past, present, future. SANS Institute publication, http://www.sans.org/reading_room/whitepapers/stenganography/ 552.php, 2001

[3] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html .

[4] Bret Dunbar, 'A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment' , SANS institute, 01/18/2002

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", *IEEE Journal of selected Areas in Communications*, May 1998

[6] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001

[7] Obaida Mohammad Awad Al-Hazaimeh, "Hiding Data in Images Using New Random Technique", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012