IMPROVING THE SECURITY OF COMPUTER NETWORKING USING STEGANOGRAPHY TECHNIQUE

Dr. B. Chellaprabha, ME., PHD

SNS College of technology, Anna University, Coimbatore

chellaprabha@gmail.com

Abstract: Nowadays the world is a global market. Every business and enterprise is related to the internet and technology in one way or the other way. Networking plays a major role in today's computer technology. But the fullest advantages are exploited only in a secured connection that is Network Security. This paper presents fundamental principles of network steganography, which is a comparatively new research subject in the part of information hiding. The main objective is to characterize network steganography which are information hiding techniques that utilize network protocols as enablers of hidden communication This method using improvising the security of network connection to prevent unauthorized access in computer network.

1. INTRODUCTION

The world is a global market today. Every business and enterprise is related to the internet and technology in one way or the other way and thus the demand for Network Security has increased many folds. Recent cases of hacking and data theft has left many organizations with no option but to hire the services of experts who can perform specific operations to check how unsafe the data is and how prone the network is to threat from data thieves. To prevent our valuable data so we need good data security techniques called as Steganography.

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages, usually steganography is applied to supplement encryption. An encrypted file can still hide information using steganography, the encrypted file is deciphered, and the hidden message is not seen.

What is Computer Network?

A computer network is a system in which computers are connected to distribute information and resources. The connection could be done as peer-to-peer or client/server. This web site reviews the techniques you can use to set up and possibly manage a network for home or a small business.

Figure 1: Example of computer Network

2. COMPUTER NETWORK SECURITY

Computer security is a branch of computer technology known as Information Security as applied to computers and networks.

The objective of computer security contains protection of information and property from corruption, theft or

natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

Why do we need security?

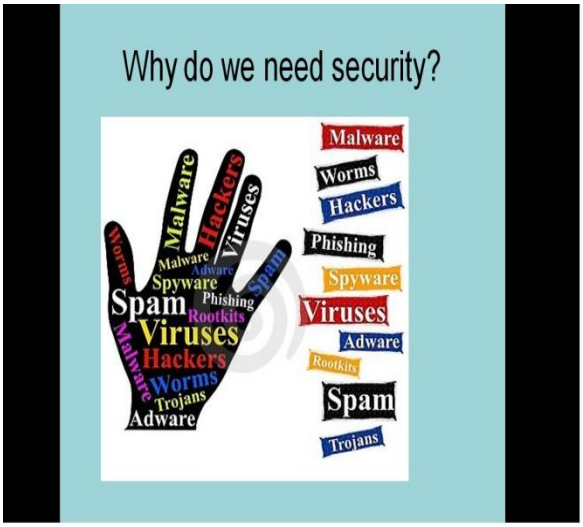

Figure 2: Type of Network attacks

Because of these,
In general, the majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has achieved access to data paths in your network to "listen in" or interpret (read) the traffic.
When an attacker is eavesdropping on your communications, it is denotes to as snooping or sniffing. The capability of an eavesdropper to check the network is normally the major security problem that administrators face in an enterprise. Internet Security along with different types of computer security and it covers hacking and malware techniques.
The Internet is an open zone where anyone can create a website that may place malware on your computer or server.

2.1 Hacker Attacks:

The term "hacker attacks" to point out hacker attacks that are not automated by programs like as viruses, worms, or Trojan horse programs, there are many forms that utilize weakness in security. Many of these may cause system crashes or loss of service.

IP spoofing

Gaining access through source routing

Figure 3: Example of Hacker

- Man in the middle attack
- Server spoofing
- Password cracking

2.2 DoS Attacks:

- **Ping broadcast**

Ping request packet is sent to a broadcast network address where there are many hosts.

- **Smurf**

An attack where a ping request is sent to a broadcast network address with the sending address spoofed. So various ping responds will come back to the victim and overload the ability of the victim to process the replies.

Figure 4: Type of Network Security

2.3 Role of steganography in Network security:

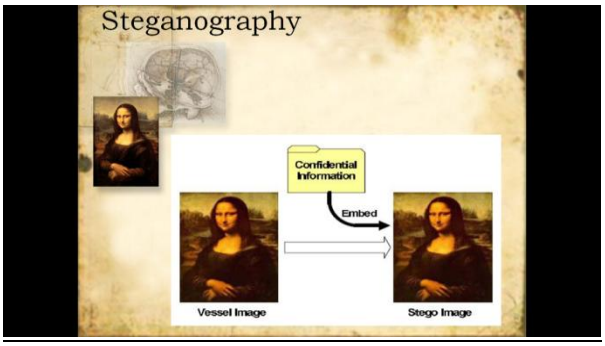

Figure 6: Example of steganography technic in image

What is it applied for?

- Hiding the detail that you are sending messages
- Hiding many messages inside data
- Digital watermarking
- Kerckhoffs' principle
- Secure with knowledge of the system
- Message can be read with secret key only.

Implementation:

Hiding Information details:

- Text or WebPages
- Images
- Audio
- Video

Text / WebPages

- Use of a codebook
- Layout of texts
- Every N^{th} character
- Make use of whitespaces and newlines
- Complex to detect and decode

Example:

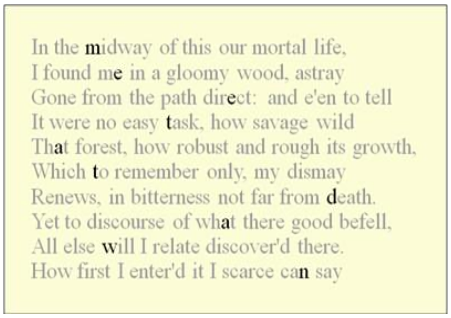

Figure 7: Example of steganography technic in Text

3. TYPES OF STEGANOGRAPHY TECHNIQUES

3.1 Physical steganography

Hidden messages are inside wax tablets —people wrote messages on the wood, in ancient Greece and in that case covered it with wax upon that innocent covering message was written.

Hidden messages on messenger body — also applied in ancient Greece. Herodotus notifies the story of a message tattooed on a slave's shaved head, exposed by shaving his head again and hidden by the growth of his hair.

During World War II, the French Resistance sent some messages written on the backs of couriers using invisible ink.

3.2 Digital steganography

The applications of digital steganography in many e-commerce applications throughout the Internet will be discussed. These applications are contains digital watermarking for digital signature authentication, copyright protection of multimedia data and validation of electronic documents, digital data storage and linkage for binding digitized photographs with personal attribute information with secure communication of multimedia data.

Figure 8: Example of Digital steganography

4. NETWORK STEGANOGRAPHY

All information hiding techniques that can be used to exchange steganograms in telecommunication networks can be classified under the common term of network steganography.

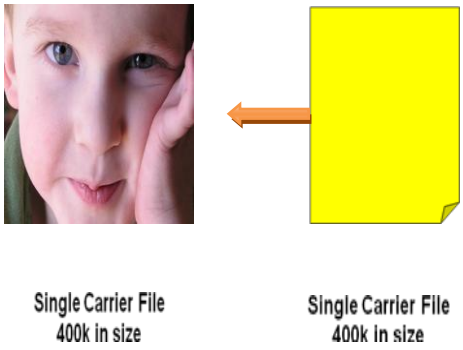

Figure 9: Example of Network steganography

The usual network steganography methods involve alteration of the properties of a single network protocol. Such modification can be applied to the PDU.

- **A simplify example with an 8-bit image**

1Pixel:

(00 01 10 11)

White red green blue

- **Insert 0011:**

(00 00 11 11)
White white blue blue

As can be seen from the example, with an 8-bit image, the cover image should be carefully chosen since LSB manipulation is not as forgiving due to the colour limitations.

- **A simplified example with a 24-bit image**

1 pixel:

(00100111 11101001 11001000)

- **Insert 101:**

(00100111 11101000 11001001)

red green blue

5. TEXT STEGANOGRAPHY

Steganography can be applied to different types of media including text, audio, image and video etc. However, text steganography is considered to be the most complex type of steganography due to lack of redundancy in text as compared to image or audio but still has smaller memory occupation and simpler communication.

Benefits of Stegnography:

- High data security
- Data integrity
- Authentication of message originator
- non-reputation

6. CONCLUSION

Covert Channels Stenography provides the means for communicating without being any noticed. That permit you to bypass normal network security methods you

can only combat covert channels if you understand how it works, steganographic tools involved hiding messages inside sound files or digital images, known as carriers, such that Thriller MP3.

REFERENCES

[1] Lubacz, J., Mazurczyk, W. and Szczypiorski, K., 2012. Principles and overview of network steganography arXiv preprint arXiv: 1207.0917

[2] Saraireh, S., 2013. A Secure Data Communication system using cryptography and steganography, International Journal of Computer Networks & Communications, 5(3), p.125

[3] Saleh, M.E., Aly, A.A. and Omara, F.A., 2016. Data Security Using Cryptography and Steganography Techniques, International Journal of Advanced Computer Science & Applications, 1(7), pp.390-397

[4] Sateesh, G., Lakshmi, E.S., Ramanamma, M., Jairam, K. and Yeswanth, A., Assured Data Communication Using Cryptography and Steganography.

[5] Mehndiratta., A., 2015. Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation.

[6] Singh, A. and Malik, S., 2013. Securing data by using cryptography with steganography, International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp.404-409

[7] Abdulzahra, H.A.Y.F.A.A., AHMAD, R. and NOOR, N.M., Combining Cryptography and Steganography for Data Hiding in Images. ACACOS, Applied Computational Science ISBN, pp.978-960