Abstract: The term steganography is described as the means to conceal secret information in honest carriers that are not aware of the existence of the secret information, which is subsequently extracted at the destination. This paper discusses the fundamental principles of network steganography that is a relatively new approach of information hiding, followed by a brief overview of various network steganography procedures and techniques.

1. Introduction

The advancement of technology, the Internet and information sharing has increased the complexity of protection of information from unsought and undesired access. Thus as the Internet has become an essential part of our daily lives it is imperative to address the issues of protection which involve confidentiality, reliability, safety, availability, anonymity, integrity etc. One of the proposed classifications for such issues is the CIA triad (Confidentiality, Integrity, Availability) [1], [2]. In this paper however we are discussing the methods of providing confidentiality in digital communication using one such method of information hiding that is steganography. Our focus is on one subset of methods of steganography that is network steganography.

Steganography is the art of information hiding in ways that prevent the detection of hidden information. Steganography derived from Greek literally means, “Covered writing” and has a long history; people have hidden information by a multitude of methods and variations [3]. In contemporary digital communications there are a number of steganographic techniques that involve hiding information in images, plain text, videos and other data transmitted between communicating parties. Steganography is not tantamount to cryptography; cryptography encrypts the message so that it cannot be understood while steganography hides the message’s very existence.

Along with the different types of media steganography, which utilize the media files, another method is the utilization of network protocols as a carrier this method is known as network steganography. Krzysztof Szczypiorski at Warsaw University Technology first introduced the term network steganography. Typically network steganographic methods use TCP/IP protocols’ control elements and their intrinsic functionality making this method difficult to detect and eliminate [4]. This method generally involves the modification of the protocol data unit (PDU), the time relations between the PDUs or both.

2. Recent Developments

Address Resolution Protocol (ARP)[7] is a protocol which operates between the data link layer and network layers of the Open Systems Interconnection (OSI) model. IP networks are used to find Media Access Control (MAC) when only IP address is known. ARP is important for any switched Local Area Network (LAN). Frame length is restricted to a minimum range of 64 octets and a maximum range of 1500 octets, in Ethernet.
Additional data needs to be padded if length is less than 64 octets.

Since Link Layer Control (LLC) is very rarely utilized in 802.3 networks, the size of an Ethernet data field should be 46 octets and filled with data originating from any upper layer protocol. There is no encapsulation done at this stage.

However, due to standardization RFC 1042 and RFC 894, implementations of padding mechanism in NICs (Network Interface Cards) drivers vary. Additionally, some drivers handle frame padding inaccurately and does not fill it with zeroes. As a result, memory leakage takes place and Ethernet frame padding contains portions of kernel memory.

This threat is added in At stake report and is called Etherleak [10]. Data which is inserted in padding is considered unlikely to contain any valuable information; therefore, it is not serious threat to network security. However, it is a perfect candidate for a carrier of steganograms. Using of padding in Ethernet frames for steganographic was put forth by Wolf [9]. It may be used to compromise network defenses. If each frame has a padding set to zeroes its usage is easy to detect. With the help of Etherleak, this information hiding scheme is attainable as it will be hard to distinguish.

3. Network Steganographic Techniques

A. SkyDe

SkyDe is the short form of the term SKYPE HIDE, which is an up and coming method for steganography. SkyDe, as the name suggests uses the software Skype to communicate in secret using the silent packets in the Skype transmission. Now as Skype does not use any mechanism for silent suppression, so it is possible to re-write the packets for the silent suppression. The packets on which this would work are the ones where there is no audio signal being transmitted. This leads to SkyDe offering higher amount of bandwidth for stenography.

Skype uses the technology of VOIP (Voice Over IP) or IP telephony. This technology allows us to place phone calls over the IP network instead of data packets. Skype is currently owned by tech giant Microsoft and is a peer to peer (P2P) telephony services. [5] (Check for sources from the paper)

As Skype provides with state of the art encryption, it can be used to send encrypted data by SkyDe instead of encrypted silence. This method makes SkyDe’s detection extremely hard and makes the data extra secure. Also SkyDe only uses 30% of all the packets with silence so as to bring better security and reduce the low voice quality distortions. [10] The bandwidth provided by SkyDe is almost 2 Kbits of steganography.

B. StegTorrent

StegTorrent is a network steganographic method which is currently new in market. StegTorrent uses BitTorrent, a popular p2p file transfer manager to encode the secret information in the data transaction. StegTorrent achieves this by using exchange protocol in peer to peer transfer. In exchange protocol it changes the order of the data packets. There are other methods require synchronization but StegTorrent does not require it. BitTorrent is a peer to peer file sharing system that allows users to send huge amount of data among themselves easily over IP networks. [6] A BitTorrent user shares either a part of data or the whole data, with so many clients that this is taken as an advantage easily by the StegTorrent. [7]

In a hidden communication scenario, the number of hidden data senders and the data receivers who are in control with BitTorrent client and their IP addresses are known to each other. The network topology can be or cannot be known as it is not a necessary requirement. The hidden sender starts to send the data using the StegTorrent client over the network. Then the resource downloaded by the another StegTorrent client is shared and this is group of BitTorrent clients in a closed group.

C. SCTP Multistreaming

Stream Control Transmission Protocol(SCTP) improves the performance by mixing TCP and UDP components. Steganograms bits are transmitted in chunks, in this method. Let the steganograms bits be 11011100 and let there be 4 streams - Stream 1, 2, 3 and 4 [11]. The steps are:

- Sender wants to transmit following hidden bits: 11011100.

- First two hidden bits are 11, so a chunk within stream 3 is sent.

- Next transmit bits 01 within a stream of 2.

- Next bits 11 are transmitted within stream 4.

- Finally bits 00 within stream 1.

D. TranSteg

TranSteg (Transcoding Steganography) is a modern IP telephony steganographic method. It compresses open data to make space for the steganograms. This can be achieved by transcoding. TranSteg retains voice quality. It offers high steganographic bandwidth. In TranSteg, the hidden information is extracted and the speech data is restored to the data originally sent. This is a brobdingnagian advantage, when the existing VoIP
steganographic methods is compared with TranSteg. In other methods, hidden data can be removed and extracted, but the original data is not restored because it has been erased during the hidden data insertion process [12]. TranSteg is intended for a broad class of multimedia and real-time applications e.g. IP telephony. TranSteg can be used in other applications or services like video streaming, where there is need for efficiently compressing the overt data.

The common approach to steganography is to compress the covert data to decrease its size [10]. TranSteg utilizes compression to make space for the steganograms of the overt data. TranSteg is using transcoding for voice data from a higher bit rate codec (overt codec) to a lower bit rate codec (covert codec) with the minimum degradation in voice quality. TranSteg functions as follows:

- Find a codec that results in a similar voice quality but smaller payload size than originally selected, for a given RTP voice stream,

- The original voice payload size is unaltered intentionally and the change of codec is not indicated. After placing the transcoded voice payload, the remaining space which is free is filled with hidden data. TranSteg detection is difficult to perform if Secure Real-time Transport Protocol (SRTP) is utilized for Real-time Transport Protocol streams.

E. PadSteg

Padding Steganography is the steganographic system for LANs. PadSteg is the first inter-protocol steganography solution. Inter-protocol means the use of relation between two or more protocols from the TCP/IP to enable communication in secret [11]. PadSteg replaces padding bits of the Ethernet frames with steganograms. Etherleak is caused by ambiguous standardization which makes the implementation of padding protocol different. The known Etherleak vulnerability makes PadSteg not easy to detect. Some NIC drivers handle frame padding incorrectly and fail to fill it with zeroes [1]. PadSteg uses Address Resolution Protocol (ARP) to identify all PadSteg hidden nodes and also perform carrier-protocol during hidden exchange. Carrier-protocol hopping is a capacity to arrange carrier-protocol of the steganograms during hidden communication. PadSteg exchanges data with short frames such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), ARP and Internet Control Message Protocol (ICMP).

Table 1. Comparison of Steganographic Method Groups. [1]

<table>
<thead>
<tr>
<th>Group of methods</th>
<th>Pros</th>
</tr>
</thead>
</table>
| Methods that modify protocol PDU/PCI | - High steganographic bandwidth  
- Easy implementation  
- No sender-receiver synchronization required |
| Methods that modify protocol PDU/SDU | - Harder to detect than PCI-based methods  
- No sender-receiver synchronization required |
| Methods that modify payload modification | - High steganographic bandwidth  
- Hard detection  
- No sender-receiver synchronization required |
| Methods that modify packet fields between PDUs | - Easy implementation  
- Hard detection |
| Hybrid methods | - Hard to detect  
- No sender-receiver synchronization required  
- High steganographic bandwidth |

4. Conclusion

Network Steganographic techniques are evolving, becoming harder to detect. New undetectable data carriers could be exploited. Data traffic of genuine internet users might also be exploited and this would have its own legal ramifications. Recently, there has been an alarming increase in the development and use of network steganographical techniques for malicious purposes. Therefore, additional research is necessary to formulate new countermeasures.

1. Acknowledgements

The authors would like to thank the faculty of Computer Engineering Department, Thadomal Shahani Engineering College, Mumbai; for their invaluable guidance and support.

2. References


