DOI: 10.20472/IAC.2018.039.010

RESUL DAŞ
Fırat University, Turkey

GURKAN TUNA
Trakya University, Turkey

A SIMPLE APPLICATION FOR NETWORK STEGONAGRAPHY

Abstract:

The Internet has changed the paradigm of traditional circuit switch network largely. The services and applications have been created by the network users themselves. This paradigm shift is one of the main sources of the tremendous success of the Internet. On the other hand, although the Internet has created many new possibilities and opportunities, communication through the Internet is subject to many security risks.

In this paper, we propose a simple application to transfer sensitive data securely and present its details. The application we propose secures the exchange of sensitive data by relying on network steganography. When the users input data at the application's interface, the data is hidden in IP packets before transmission so that it cannot be obtained by malicious users. Since the required libraries are more stable and can be easily found on the Linux platform, the application was developed for the Linux platform.

Keywords:

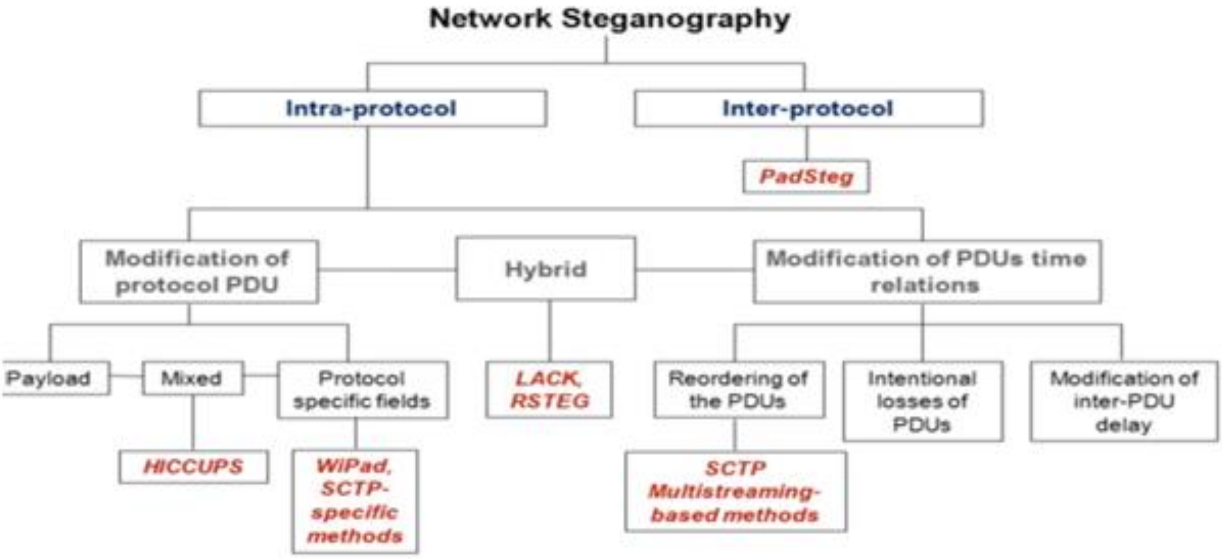
Sensitive data, Data confidentiality, Steganography, Application.

JEL Classification: L86, C88

1 Introduction

Although in the last couple of decades, especially in recent years, the Internet has created many opportunities and started to reduce communication costs significantly. However, due to its nature and being a public communications network, Internet applications and communications over the Internet infrastructure are subject to many information security threats (Jung, Han, and Lee, 2001). Though these threats were not taken into consideration in the past, nowadays people are aware of these threats because of various malicious attacks occurred in recent years. Due to the increasing awareness, solutions have been developed to secure communications over the Internet. One of the solutions to this problem is steganography, the name given to the science of hiding information (Zielińska, Mazurczyk, and Szczypiorski, 2014). The word steganography was derived from the Greek (Mishra and Bhanodiya, 2015). Thanks to various steganographic techniques, sensitive data can be kept confidential and be shared with only authorized users. By hiding data into packets, network steganography allows facilitating the process of sending sensitive data over a public communications network such as the Internet (Lubacz, Mazurczyk, and Szczypiorski, 2014). Figure 1 shows a classification of intra-protocol and inter-protocol network steganography techniques.

Figure 1: Classification of network steganography techniques (Lubacz, Mazurczyk, and Szczypiorski, 2014; Mazurczyk, et al., 2016; Bender, 1996; Kundur and Ahsan, 2003).


Network Steganography
Intra-protocol
Inter-protocol
PadSteg
Modification of protocol PDU
Hybrid
Modification of PDUs time relations
Payload
Mixed
Protocol specific fields
LACK, RSTEG
Reordering of the PDUs
Intentional losses of PDUs
Modification of inter-PDU delay
HICCUPS
WiPad, SCTP-specific methods
SCTP Multistreaming-based methods

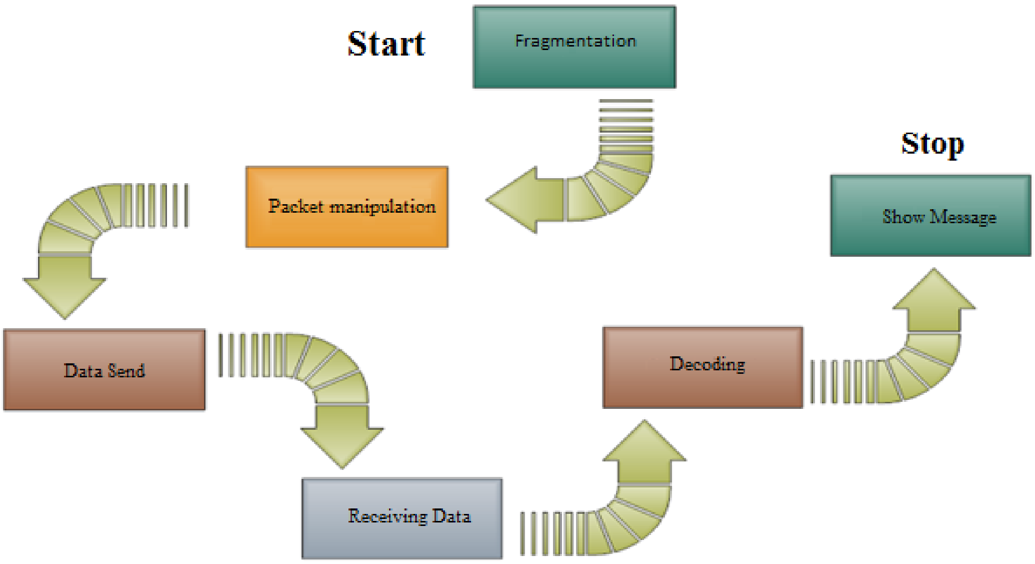
The typical network steganography method uses a single network protocol change. The protocol change can be applied to the Protocol Data Unit (PDU), the time relationships between the modified PDUs, or both (hybrid) (Lubacz, Mazurczyk, and Szczypiorski, 2014). It is also possible to use an association between two or more different network protocols to establish confidential communication. This is called inter-protocol steganography. Within each TCP header there are many fields that are not used for normal transmission, or "optional" fields are set by the sender of the data networks as needed (Kozierok, 2005). The analysis of unused or optional fields of a typical IP header reveals many possibilities that the data can be stored and transmitted. Since some fields are sometimes altered or stripped by packet filtering mechanisms or fragment reassembly (Stevens, 1993), we focus on TCP start sequence number field (Sequence Number Field) and IP Identification Field.

2 Proposed Application

Since many business processes and personal applications rely on the infrastructure of the Internet, we need to develop applications to provide data communications securely. Therefore, the proposed application was designed to transfer sensitive data securely over public communications networks such as the Internet. Main advantages of the proposed applications are easy installation, simple design and ease of use. The drawback of the proposed application is that it is operating system dependent and only runs on Linux distributions.

In the proposed application, TCP start sequence number field (Sequence Number Field) and IP Identification Field are used to hide sensitive data. The basis of exploitation is based on coding the ASCII values. In the development process, Standard C/C++ Library, Linux-IP/Linux-TCP Library, QtCreator Form Library, Netinet Library and Boost Library have been used. Figure 2 shows the flow of the process of the proposed application and Pseudo Code of the application is listed below. First, the fragmentation of the message content is performed. Then, the fragmented contents are manipulated and sent to the Data Send queue. The packets send by the queue are listened in Server mode and as soon as they are received, they are sent to the Decoding queue. Then, they are decoded by the related functions and their contents are displayed. Detailed flow of the processes is shown in Figure 3.

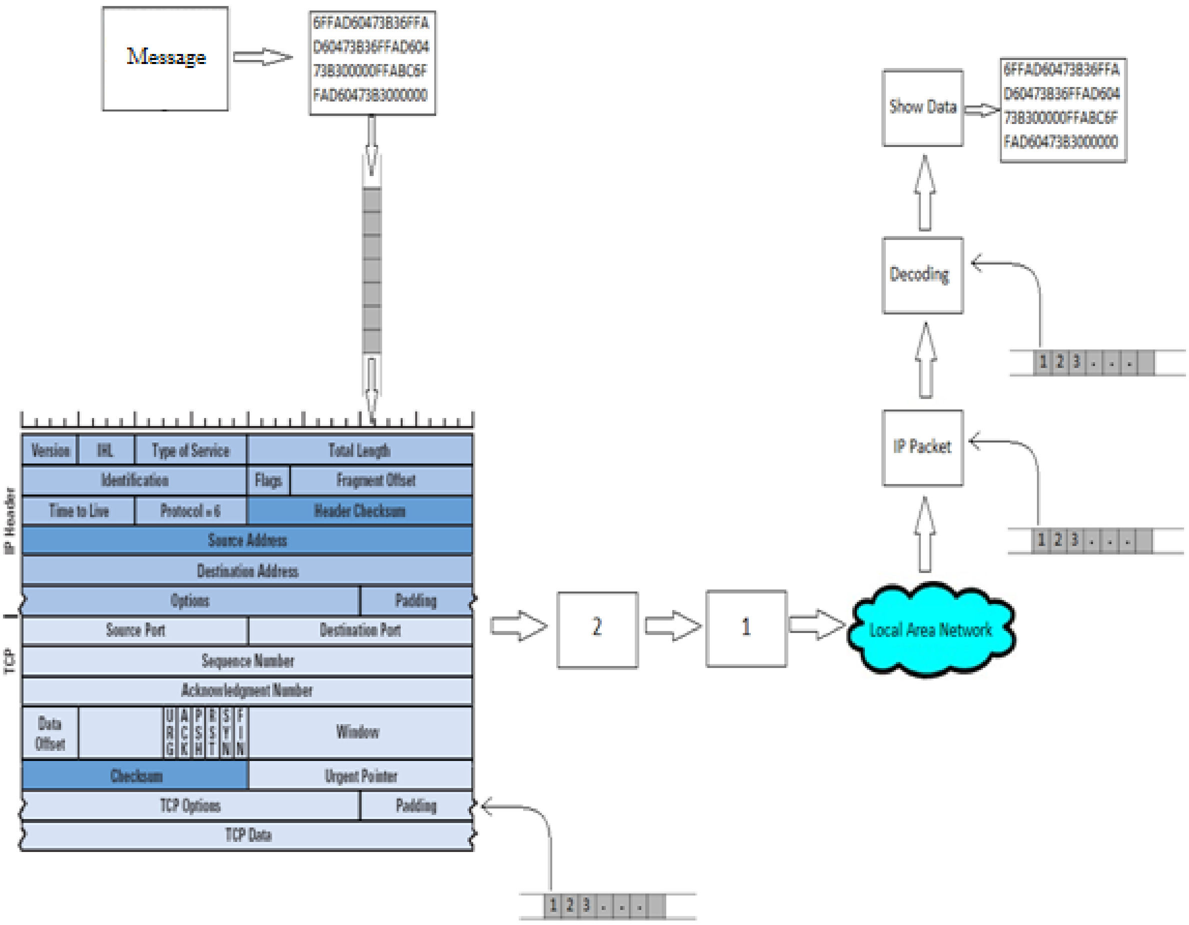
Figure 2: Flow of the processes of the proposed application



Pseudo Code of the application

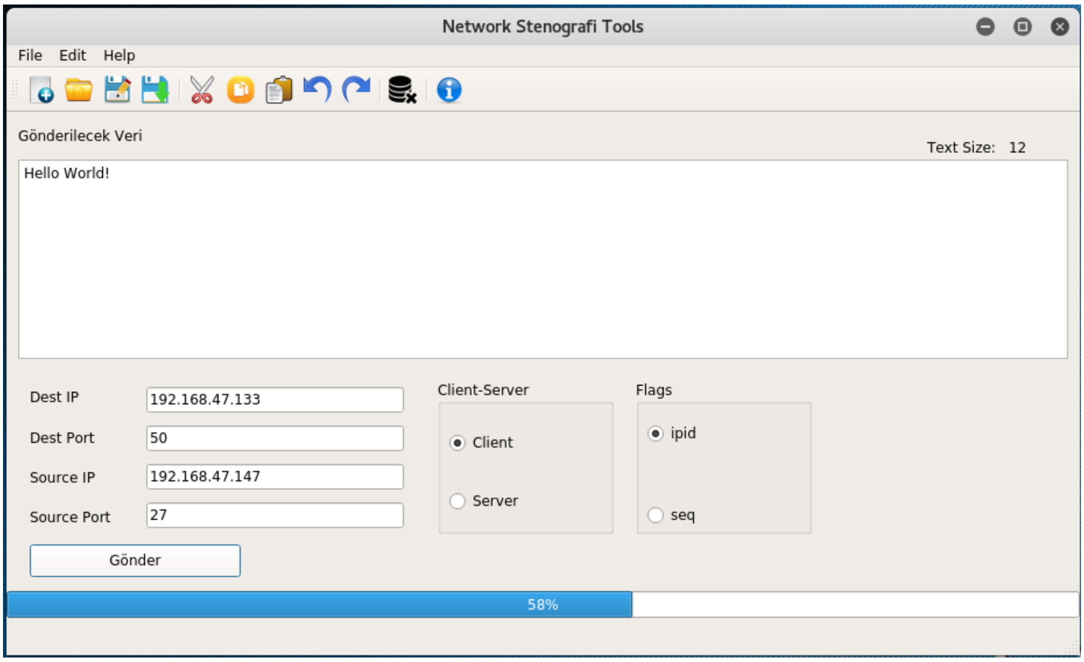
```
If (if root does not exist)
        Warning, "You need root privileges to run this application."
End if
      Target_host <- enter;
      Source_host <- enter;
      Source_port = <- enter;
      Source_port <- enter;
      Target_host = host translate to ip number (hostname);
      Source_host = host translate to ip number (hostname);
      Package_create (flags, client, server);
      Package_encrypt;
      Package_render (source_host, destination_host, source_port, destination_port);
      Package_al (source_host, destination_host, source_port, destination_port);
      Decrypt package;
      Show the data;
End if
```

Figure 3: Detailed flow of the processes



The application was designed to facilitate the process of sending confidential data. The application's graphical user interfaces are shown in Figures 4 and 5. If the user aims to send a message to a client or aims to receive a message from another client, the client radio button is selected. A flag must be selected, too. After selecting the flag, the user can select the source IP address, source port number, destination IP address, destination port number, and then can send the message in a text file to the other client either by opening it from the File menu or by clicking on the open icon from the toolbar. After finishing the selection or write operation, the message must be saved and then clicking on the Send button it can be sent.

Figure 4: The application in the client mode



Gönderilecek Veri

Text Size: 12

Hello World!

Dest IP: 192.168.47.133

Dest Port: 50

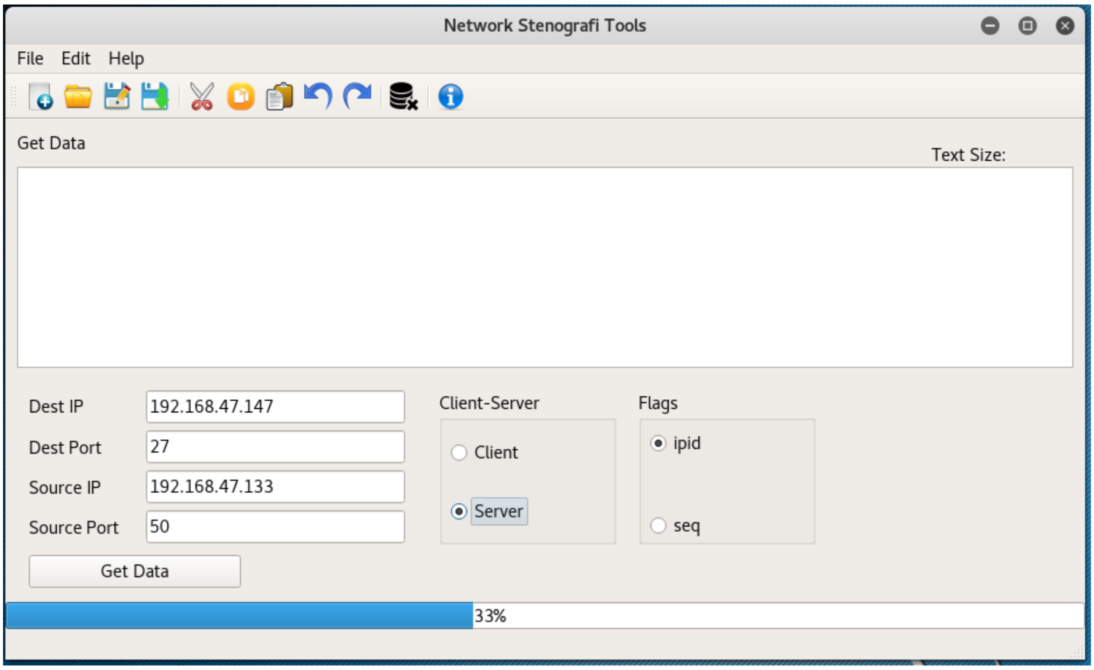
Source IP: 192.168.47.147

Source Port: 27

Client-Server: ● Client ○ Server

Flags: ● ipid ○ seq

Figure 5: The application in the server mode



Get Data

Text Size:

Dest IP: 192.168.47.147

Dest Port: 27

Source IP: 192.168.47.133

Source Port: 50

Client-Server: ○ Client ● Server

Flags: ● ipid ○ seq

In order to receive a message from another client, the user needs to know the following three pieces of information: the IP address and port number of the other party, and the port to be used to receive the message. If this information is available, the user can enter the source IP address after selecting the server radio button. After writing the source IP address of the other party in the target host section, the source port address of the other party in the target port section, and the port number to be used to receive the message, the user can start receiving the message.

3 Conclusion

Although the Internet has changed the paradigm of how business processes operate and how people communicate and offers many benefits, due to its public communications network, there are many information security risks. Accordingly, in this paper, a simple application was proposed and developed to exchange sensitive data securely. The application relies on network steganography and helps to secure the exchange of sensitive data. When the users input data at the application's interface, the data is hidden in IP packets before transmission so that it cannot be revealed by malicious users. Since the required libraries are more stable and can be easily found on the Linux platform, the application was developed for the Linux platform.

References

Bender, W. (1996). Techniques for Data Hiding. *IBM System J.*, 35(3-4), pp. 313-336.

Jung, B., Han, I., and Lee, S. (2001). Security threats to Internet: a Korean multi-industry investigation. *Information & Management*, 38(8), pp. 487-498.

Kozierok, C. M. (2005). *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference,* 1st Edition, No Starch Press, San Francisco, CA.

Kundur, D. and Ahsan, K. (2003). Practical Internet Steganography: Data Hiding in IP. *Proc. Texas Wksp. Security of Information Systems*.

Lubacz, J., Mazurczyk, W., and Szczypiorski, K. (2014). Principles and overview of network steganography. *IEEE Communications Magazine*, 52(5), pp. 225-229.

Mazurczyk, W., Wendzel, S., Zander, S., Houmansadr, A., and Szczypiorski, K. (2016). *Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures*, Wiley-IEEE Press.

Mishra, R. and Bhanodiya, P. (2015). A review on steganography and cryptography. *2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)*, Ghaziabad, India.

Stevens, W. R. (1993). *TCP/IP Illustrated, Vol. 1: The Protocols*, 1st Edition, Addison-Wesley Professional.

Zielińska, E., Mazurczyk, W., and Szczypiorski, K. (2014). Trends in steganography. *Communications of the ACM*, 57(3), pp. 86-95.