ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Data Hiding Using Steganography For Network Security

Rupali Gawade[1], Priyanka Shetye[2], Vaibhavi Bhosale[3], P N. Sawantdesai[4]

Student, Computer, Rajendra Mane College of Engineering & Technology, Ambav, India[1,2,3]

Assistant Professor, Computer, Rajendra Mane College of Engineering & Technology, Ambav, India[4]

Abstract: This work relates the areas of steganography, network protocols and security for data hiding in communication networks employing TCP/IP. Steganography is defined as the art and science of hiding information, which is a process that involves hiding a message in an appropriate carrier for example an image file or IP Header. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. In this project we present a scheme to send message imperceptibly between points over Internet using any encryption algorithm which is used to encrypt secret message, and then embeds the modulated message into identification field of IP header. This thesis investigates the existence of covert channels in computer networks by analysing the transport and the Internet layers of the TCP/IP protocol suite. Two approaches for data hiding are identified: packet header manipulation and packet sorting. The packet sorting approach is simulated at the network layer which provides a feasibility of packet sorting under varying network conditions. While bridging the areas of data hiding, network protocols and network security, both techniques have potential for practical data hiding at the transport and network layers.

Keywords: Steganography; Cryptography; TCP/IP; RSA.

I. INTRODUCTION

As the Internet permeates our daily lives, there is a need to address issues of protection; flexible security for evolving network applications is required. This work attempts to integrate traditional network security with another emerging technology, data hiding. Many forms of information hiding such as encryption are used for data hiding, where both parties encrypt the information and transfer a cipher. These techniques have become much more open and public in the last few years. The steganography aims to prevent a third party from realizing that any covert communication has taken place better than the encryption Steganography is defined as the art and science of hiding information, transmitting secret messages through innocuous cover carriers in such a manner that the existence of the embedded messages is undetectable. Only persons who have knowledge of the embedded information and possess a "key" will be able to decode and view the information. This key can take many forms. It can range from a passphrase for electronic stegnography to an understanding of a method to decode the information

A. Steganography:

In this paper we, are going to discuss about steganography, it is defined as the art and science of hiding information, which is a process that involves hiding a message in an appropriate carrier for example an text file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. Steganography is a general term referring to all methods for the embedding of additional content into some form of carrier the choice of the carrier is nearly unlimited; it may be an ancient piece of parchment, as well as a network protocol header. Present day steganographic methods are far more sophisticated than their ancient predecessors, but the main principles had remained unchanged. They typically rely on the utilization of digital media files or network protocols as a carrier, in which secret data is embedded. Steganography is a general term referring to all methods for the embedding of additional secret content into some form of carrier, with the aim of concealment of the introduced alterations. The choice of the carrier is nearly unlimited; it may be an ancient piece of parchment, as well as a network protocol header. Inspired by biological phenomena, adopted by man in the ancient times, it has been developed over the ages. Present day steganographic methods are far more sophisticated than their ancient predecessors, but the main principles have remained unchanged. They typically rely on the utilization of digital media files or network protocols as a carrier, in which secret data is embedded.

B. cryptography:

Cryptography is a method of storing and transmitting data in a form so that it can no more be interpreted or understood. It is a science of protecting effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths.

i. How does cryptography works:

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key –a word, number, or phrase- to encrypt the plaintext . the same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work, comprise a cryptosystem.

ii. Encryption:

The process of converting plain text into cipher text using appropriate key.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

iii. Decryption:
The process of converting cipher text into plain text using an appropriate key.

C. RSA Algorithm (Rivest-Shamir-Adleman) **:**
RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security.

i. How RSA system works:
The mathematical details of the algorithm used in obtaining the public and private keys. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet.

The private key is used to decrypt text that has been encrypted with the public key. Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it. A table might help us remember this.

II. EXISTING SYSTEM

The traditional approach encrypts the data in the Application layer e.g. HTTP protocol, the most popular and common protocol used over the Internet, uses SSL (Secured Socket Layer)technique for encryption and decryption of data send over the Internet. It uses 1 28 bit Cipher Lock, supported by latest Internet Browsers like Internet Explorer (IE 6.0 & above), Netscape Navigator 7.0 & above, and Web Servers like IIS (Internet Information Server (Microsoft only)),Apache, Tomcat etc

III. PROBLEM DEFINITION

Problem statement
"In this project we are sending the data from sender to receiver in hidden format using cryptography and steganography techniques."

IV. SCOPE OF RPOJECT

Network Security is of the most active research areas today. To address security issues, one needs to have a comprehensive understanding of the available framework as well as all the aspects connected with the same. This thesis attempts to cover a comprehensive picture. The breadth of the work includes data communication in networks, relating data hiding concepts (mainly associated with digital images) to network packets, the TCP/IP protocols' analysis, network security mechanisms like firewalls and the security architecture of the Internet Protocol. It primarily aims to provide some security means to standard network protocols and security procedures by effectively utilizing the available

V. PROPOSED SYSTEM

Two approaches for data hiding are identified: packet header manipulation and packet sorting. The packet sorting approach is simulated at the network layer which provides a feasibility of packet sorting under varying network conditions. While bridging the areas of data hiding, network protocols and network security, both techniques have potential for practical data hiding at the transport and network layers.

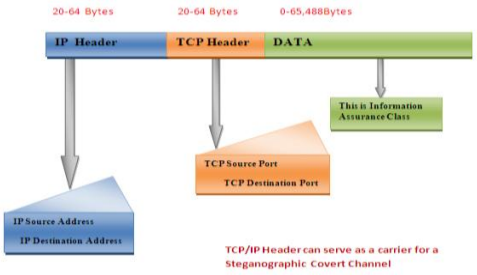

Fig.1. TCP/IP Header can serve as a carrier for a Steganographic Covert Channel

A. Methodology

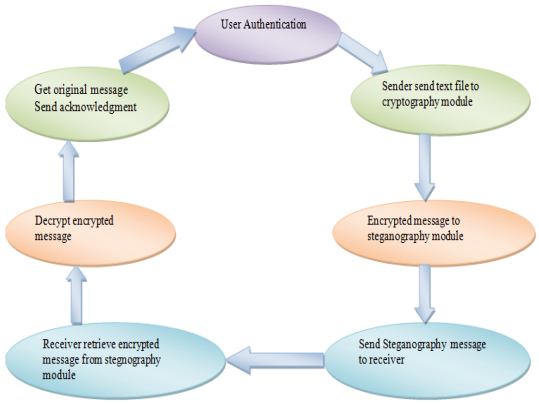

Fig . 2.Methodology of file transmission & reception

Description

Step 1: Authentication of both parties.
Step 2: Sender decide to send text file to the receiver.
Step 3: Text file is sent first to the encryption module .
Step 4: Encrypted message is sent to the steganography module.
Step 5: Receiver retrieves the encrypted message from steganography module which is sent by the sender.
Step 6: The encrypted message is decrypted and original message is retrieved.
Step 7: Acknowledgement is sent to the receiver

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

B.Modules of the Application

The tool mainly implements following modules.

1. *Steganography module:*

Steganographic module consist of a forth order chaotic method for packet sequence generation. Using this method the data is hidden into identification field of IPv4 using chaotic mixing. Identification field carries a value assign by sender to aid in assembling the fragment of datagram at receiver.

- The Forth Order Chaotic Method For Packet Sequence Generation

A fourth-order Chebyshev chaotic system can be described by a simple mathematical equation as following [7]:

Xn+l = cos (4arccos xn),xn € (- 1 , 1) ..... [1]

Given a value of x0,one can generate a specific sequence from an initial using equation 4.

In order to enhance random city and meet our use as well, we need to convert the chaotic sequence to binary sequence.

The convert function is equation S.

M(X) = 1 , X >= 0

- 1 , X < 0 ..... [2]

Suppose x0=0.15, after iterative for 500 times (n=500), we get a chaotic sequence (as upper). After convert, we get a binary sequence.

Thus the secret key will be a type of combinatorial x0 and n.

For example, the key may be:

Key =x0 ExOR n ..... [3]

The strength of a data hiding scheme depends on its non detectability either by the administrator or by any automated network-monitoring scheme; its identification field appears to be perfectly "normal". Chaotic mixing provides structured scrambling. Compared with Toral Auto orphism System, it can provide higher random city and higher security.

- Indication Of Packets Order

We can use a simple method to identify the packets order. Suppose we embed message into IP identification field. This field has 1 6 bits, the first 8 bits can be used to carry message and the next 8 bits can be used to identify the order. For example, if we want send text "ABCDEFGH" to someone, ASCII value for B is 66 and its binary equivalent is OJ 0000 1 0, ASCII equivalent of H is 72 and the binary representation of 72 is 1 00 1 000. Packet 2 will carry B and packet 8 will carry H.

So ID field of packet 2 will be 0 1 0000 I 0 000000 I 0 and ID field of packet 8 will be 1 00 1 000 0000 1 000. When these packets arrive, receiver knows that B should be placed at the second position and H should be placed at 8th.This method will narrow bandwidth, but it's a balance between complexity and bandwidth. We assume that our communicating parties denoted as Alice (sender) and Bob (receiver) , transfer information overtly over a computer network, and employ data hiding involving the TCP/IP protocol suite to communicate supplementary information covertly.

Alice's End

Alice performs the following operations to encode a covert data symbol:

Step 1. Use PLPMTUD to determine the path MTU.

Step 2. Choose an initial x0 and n to generate a chaotic sequence Kn. The secret key is generated by equation 6. Bob is told to use this key to extract secret information. Then divide Kn into groups (1 6bit/group) and get {K1, K2, ... , Kk} in the right order

Step 3. Convert secret message into binary sequence Mn and divide it into groups (8bit/group). Per group will be padded with its group number (its binary equivalent, 8 bit). We can get {M1, M2 ... Mk}.

Step 4. Use {KI, K2, ... , Kk} to encrypt {MI,M2, ... , Mk}.

We can get covert information {Ck}:

Ci = Mi ExOR Ki, (i= 1 , 2, ... , k).

Step 5. Select k packets {P1, P2 ... Pd and embed Ci into Pi's identification field (i=l, 2 ... k). We can get stego-network packets {Sk}

Step 6. Send {Sk} to Bob.

- Bob's End

Bob can use the key that Alice told him to generate the same chaotic sequence Kn and then divide it into {K1,K2, ... , Kk} same as Alice. To decode the secret message he can use an exhaustive algorithm. Suppose Bob receive k packets. So all these packets have k! Permutations. Combine identification fields of all received packets according to the permutations and each permutation can generate a binary sequence {C1*, C2* ... Ck*}. Decrypt {C1*, C2* ... Ck*} and get binary sequence of middle result as {T1, T2, ... , Tk}

Ti – Ci* ExOR Ki (i = 1,2,3,---k) ..... [7]

Convert the last 8 bit of every Ti into normal style. If we can get legitimate and sequential numbers, we can assert that we get the right packets order. Otherwise, try the next permutation. After determine the right order of arrival packets, Bob can extract the right secret message according

2. *Cryptography module:*

Cryptography Module consist of RSA algorithm.

3. *Client module:*

At sender side the message is first encrypted using RSA algorithm. Then this message is hidden into identification field of TCP/IP header using forth order chaotic method for packet sequence generation.

4. *Server module:*

At server side by using the secret key that is used by sender and the right arrival of packet order as that of the sender, it retrieves the encrypted message . Now this encrypted message is decrypted using the RSA algorithm i.e. using its own private key.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

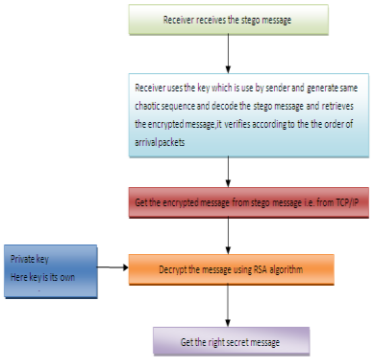

Fig. 3. At receiver side

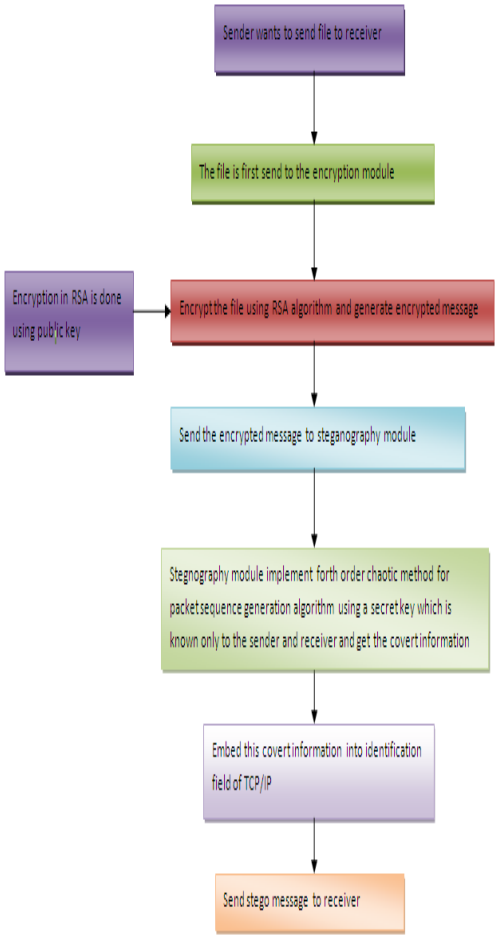

Fig. 4.At sender side

VI. CONCLUSION

Steganography is a fascinating and effective method of hiding data that has been used throughout history. Methods that can be employed to uncover such devious tactics, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect. The more that you know about its features and functionality, the more ahead you will be in the game.

Future Work

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Steganalysis. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this.

REFERENCES

[1] S.J. Murdoch, S. Lewis University of Cambridge, United Kingdom 7thlriformation Hiding Workshop, June 2005
[2] R. J. Anderson and A. P. Petitcolas, "On the limits of steganography" IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 474--481, May 1998.
[3] D. K. Kamran Ahsan. Practical Data Hiding in TCP/IP. Proc. Workshop on Multimedia Security at ACM Multimedia, 2002
[4] U S. C Information Sciences Institute, "Internet protocol, darpa internet program, protocol specification," September 1981.Specification prepared for Defense Advanced Research Projects Agency.
[5] ZHANG lie etc. "Information hiding in TCPIIP based on chaos".Journal on Communication.voJ.26 NO. I A January 2005.
[6] Steven 1. Murdoc and Stephen Lewis, "Embedding Covert Channelsinto TCP/IP". Information Hiding Workshop 2005 proceedings on, 2005