International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 10 (2013), pp. 1101-1106

http://www. irphouse.com /ijict.htm

Combating Packet Sniffing

Vineet Mishra[1], Snigdha S. Parthan[2], Sayalee Pote[3] and Naman Avasthi[4]

Computer Engineering Department, Fr. C. Rodrigues Institute of Technology, University of Mumbai, Navi Mumbai, India,

Abstract

For years, computer-network administrators have used packet sniffers to monitor their networks to diagnose and solve problems. However, sniffers today have the potential to cause personal harm because they allow a hacker to confiscate confidential information. Organisations cannot afford inside agents to sniff out important data which could harm their business. Despite the existing encryption algorithms used to tackle this problem, sniffing is a major concern. This paper adds a new perspective by proposing to use the concept of fake packets along with the existing ciphers.

Keywords: Sniffing; Security; Fake Packets; Encryption; Cryptography.

1. Introduction

Sniffing tools which were once used by System Administrators for monitoring networks are now used by hackers and script-kiddies for eavesdropping. We have entered an era where security holds more importance than data. Civil Libertarians are pressing for the widespread use of cryptography in order to protect the privacy of the individual. Arguing alongside them are businesses that require strong cryptography in order to guarantee the security of transactions within the fast growing world of Internet commerce. [1]Since the social lives of individuals are going digital, thanks to the increased craze for social networking, it is of utmost importance to safeguard these details.

2. Existing Scenario

Internet is a global collection of networks. Communication between different system users over such networks is referred to as Data transmission. There are several stages before a message from one system is successfully received by the other over this complex network.

2.1 Computer Network

Every computer that is connected to the Internet is a part of a network. One may use a modem and dial a local number to connect to an ***Internet Service Provider***(ISP). When the user connects to his/her ISP, the user becomes a part of their network. The ISP may then connect to a larger network and become part of that network. The Internet is simply a network of networks.

When two computers in this network need to communicate with each other, a *three way handshake* technique is used to establish a connection.

2.2 Three Way Handshaking Technique

The three way handshaking technique came into effect so that two computers wanting to communicate with each other can negotiate the parameters of the network connection like encryption and decryption keys, web browser requests, etc.

This technique is often referred to as "SYN, SYN-ACK, ACK" because there are three message transmitted by TCP to negotiate and start a TCP session between two computers as follows:

- Host A sends a SYN (Synchronize) packet to Host B and Host B receives A's SYN. (Figure.1)
- Host B sends a SYN-ACK (Synchronize-Acknowledgment) and Host A receives B's SYN-ACK.(Figure.1)
- Host A sends ACK (Acknowledge) which is received by Host B. (Figure. 1)
- TCP socket connection is *ESTABLISHED.*(Figure. 2)

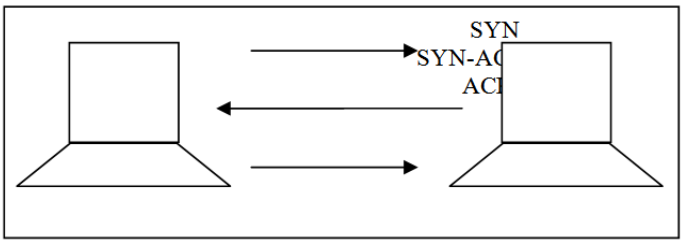

Figure 1

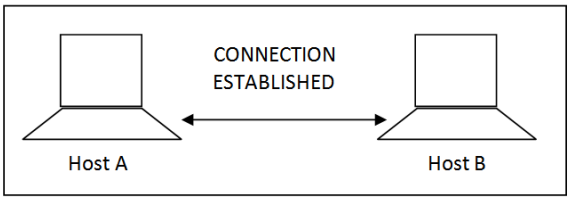

Figure 2

Once the connection is established, the data transmission can start right away. Data is transmitted over a network in the form of packets.

2.3 Packet Data

Any message that is to be transmitted from one host to another is divided into a number of parts called packets. Everything that is done on the Internet involves *packets* i.e. every message that is received comes as a series of packets and every message that is sent leaves as a series of packets.

2.3.1. Network Packet Structure:

Most network packets are split into three parts:

1. *Header:* The header contains instruction about the data carried by the packet like the length of the packet, sequence number of the packet, destination address and source address. (Figure. 3)
2. *Payload:* Payload, also called the body of the packet, is the actual data that the packet is delivering to the destination which is only a part of the message to be delivered.
3. *Trailer:*The trailer, also called *the footer*, contains a special bit pattern that tells the receiver that it has reached the end of the packet. It also contains some type of error checking code like hamming code, Cyclic Redundancy Check (CRC), etc for error detection in the transmitted data. [2]

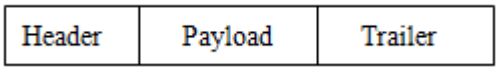

Figure 3

Each such packet that is released from its source is then directed to its destination by the best available route i.e. a route that might be taken by all the other packets in the message or by none of the other packets in the message. This applies to both wired and wireless networks.

Now, this data sent in the form of packets is prone to a lot of threats as it travels from its source to the destination. The high vulnerability of the data packet to unethical hacking and data theft led to the introduction of Cryptography in secure Data Transmission. That is, the data to be transmitted is first encrypted using various

encryption algorithms and then sent across the network. Thus the payload that we talk about is actually the encrypted data and not the pure form of data.

2.4. Cryptography

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. [3]

2.5. Public Key Cryptography

Also known as asymmetric cryptography, public-key cryptography refers to a cryptographic algorithm which requires two separate keys: public key and private key. The former is used to create a digital signature while the latter is used to verify (or authenticate) a digital signature. These pair of keys is mathematically linked to each other, each inverse of the other. Symmetric cryptography relies on one key for both encryption and decryption. However, in an asymmetric system, as the name suggests, different keys are used to perform these opposite functions.

Public-key algorithms are based on mathematical problems which currently admit no efficient solution that are inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is easy for a user to generate their public and private key-pair and to use them for encryption and decryption. The public key is widely distributed, while the private key is known only to its proprietor. The strength lies in the fact that it is either impossible or prohibitively expensive for a properly generated private key to be determined from its corresponding public key. Thus, the public key may be published without compromising security, whereas the private key must not be revealed to anyone not authorized to read messages or perform digital signatures. Awareness of the algorithm, either of the keys and samples of cipher text must be insufficient to determine the other key. [4]

The plain text is encrypted on the sender's side with the use of sender's private key. This is encrypted again, using the receiver's public key. The final cipher text can be decrypted only by the authorized receiver, who alone has the matching private key. Thus, confidentiality is provided.

2.6. Packet Sniffing

Normally, a computer only looks at packets addressed to it and ignores the rest of the traffic on the network. But when a packet sniffer is set up on a computer, the sniffer's network interface is set to promiscuous mode. This means that it is looking at everything that comes through. Packets that contain targeted data are copied onto the hard disk as they pass through. These copies can then be analyzed carefully for specific information or patterns. Once the pattern is recognized the encryption key becomes known to the sniffer and the cipher text can be decrypted. Thus, inspite of

cryptographic encryptions, the fact that the pattern from all the collected packets was recognized can lead to data theft (both ethical and unethical).[5]

3. Problem Statement

Packet sniffing can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. However, it is largely an internal threat in most organizations. In sniffing, a malicious third party may be able to eavesdrop as well as manipulate sensitive data during communication between machines in a LAN. Packet sniffing tools, which are powerful softwares, can prove to be devastating hacking tools. Even worse, these are freely available on the Internet. Some examples include Dsniff and ScoopLM. Businesses are switching ageing hubs with new switches. [6] However, packet sniffing in a switched environment, though more challenging than in a non-switched environment, is also possible. To combat this problem, our paper proposes to use the concept of fake packets along with the existing ciphers.

4. Our proposed IDEA

We propose the use of fake packets in order to increase the level of security. For each original packet, '*n*' fake packets shall be transmitted, as shown in Figure.4.Each packet may have a different key for encryption. The main idea behind malicious sniffing is to capture packets aimed to a particular destination and store them at a place. Eventually the software tries to find a pattern in the stored encrypted messages via various known methods. Once a correct key is found, the sniffer gets the actual decrypted messages which can be used for various vicious purposes.

The idea behind using fake packets is to bamboozle the sniffer. These fake packets shall also be destined to the same destination. Since the sniffer shall collect all the packets destined to a particular IP address, it shall end up storing these fake packets too. The fake packets shall carry messages taken from random sources which are completely unrelated to the communication and encrypted using different random keys (for instance encrypted texts of a classic novel).

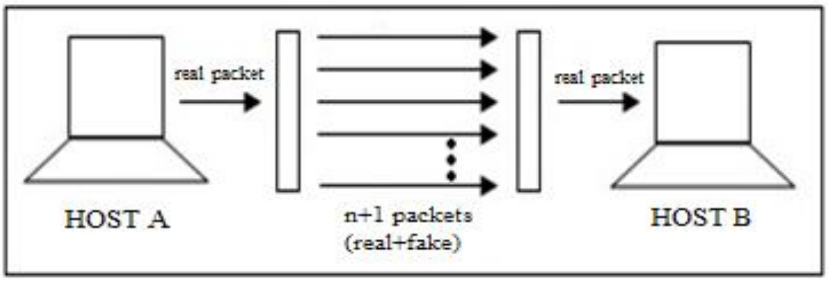

Figure 4

When the sniffing tool tries to perform decryption, it will be misled since it doesn't know the real packet amongst the fake ones and the time taken by the sniffer to find the actual set of packets will be increased massively.

At the receiver's end, when the three way handshake is established, the sender & receiver will agree upon a key and an identification index. The format of the packets needs to be modified so that we have an additional field. This additional field shall consist of an identification index (Figure.5).The distinguishing property of these identification indexes is their uniqueness. When all the packets (real and fake) arrive at the receiver's end the receiver shall accept only the packet whose identification index matches the pre decided one. The packets whose identification index does not match (i.e. fake ones) are dropped.

Figure 5

The use of fake packets may cause strain on traffic on the network. But this condition can be alleviated by using efficient algorithms. Therefore, this proposed mechanism ensures increased security.

5. Conclusion

This paper explains the existing scenario of communication between systems in a network and the data packets. Second section explains the process of public key cryptography. On this basis, we propose an idea stressing on the use of fake packets for transmission along with the packet containing the real payload to intensify security.

References

[1] Simon Singh (2000),*The Code Book*, Fourth Estate Limited
[2] http://computer.howstuffworks.com/question5252.html
[3] http://www.webopedia.com/TERM/C/cryptography.html
[4] WilliamStallings (2005), *Cryptography and Network Security 4th Ed*, Prentice Hall
[5] http://cmputer.howstuffworks.com/workplace-surveillance2.html
[6] Tom King (2002),*Packet Sniffing in a Switched Environment*,SANS Institute InfoSec Reading Room