A Novel Solution for IP Spoofing Attacks

Asma Basharat, Rabia Sirhindi, Ahmad Raza Cheema and Imtiaz Khokhar
Information Security Department, College of Signals
National University of Sciences and Technology
Pakistan

Abstract: IP spoofing is one of the most common forms of on-line disguise. Hackers have long employed the tactic of disguising their true identity. It exploits the security weaknesses in TCP/IP protocol suite. This paper evaluates basic techniques to exploit vulnerabilities of TCP/IP protocol suite such as initial sequence number prediction and forging the source address. This paper covers certain threats and attack methods that employ IP spoofing and analyze preventive measures such as ingress and egress filtering at routers, authentication and encryption.

Keywords: Spoofing, TCP, IP, filtering, authentication, encryption, sequence number prediction.

1 INTRODUCTION

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the most widely used protocol suite. It provides specifications for the communication of different computer systems across a communication network. It has been developed in the 1970's for the use on ARPA networks by the Department of Defense. The TCP/IP suite is a group of protocols that perform different functionalities on different logical layers during communication. The four logical layers are the Link Layer, Network Layer, Transport Layer and the Application Layer [1]. We will focus on the network and the transport layer. The network layer is responsible for the communication between hosts. Its basic functions are routing and forwarding of information and data packets. The transport layer protocol provides logical communication between application processes running on different hosts. However there are a number of security weaknesses inherent to its fundamental specification. Two of the weaknesses discussed in this paper are found in the TCP/IP [2][3].

IP is implemented at the network layer. It provides details for the communication between the hosts. IP is a connectionless protocol that provides best effort service for the delivery of packets across the Internet. The fields of our interest in the IP header are the source and destination IP addresses (Fig.1.). The main security flaw lies with in these fields. The contents of these fields can easily be modified using attack tools. The attacker can forge the source address, as the machine IP addresses are not checked for authenticity [4].

TCP is a connection oriented protocol implemented at the Transport Layer. The participating hosts are required to establish a connection before any transmission can take place. A three-way handshake is used to establish a network connection. The sender requests a connection by

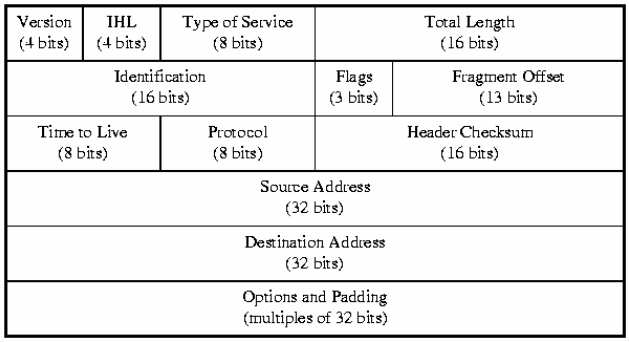

Fig.1. IP header

sending a SYN packet with its initial sequence number (ISN). The receiver responds by sending back a SYN packet with its ISN and acknowledging the sender's ISN. Finally the sender acknowledges the receiver's ISN and connection are established for the transmission of information [2].

The sequence number (SN) and acknowledgement number (AN) fields are important for in-order and reliable delivery of data. These fields ensure data delivery and determine whether the data needs to be retransmitted or not. The SN is counted byte per byte. It is the first byte in the current packet and it gives the number of next byte to be sent. AN is the next expected SN in the stream. This relationship confirms on both ends that proper packets are being received.

The paper is organized as follows. Section 2 describes two main types of IP spoofing and Section 3 covers major attack types that employ IP spoofing. Existing defense mechanisms against spoofing are discussed in Section 4 while a potential solution involving changes to the existing information in the IP header is proposed in Section 5. Section 6 explores future considerations.

2 SPOOFING ATTACKS

Spoofing attacks are used by hackers and unauthorized users to hide their original identity. There are two basic types of spoofing attacks which are used by majority of the hackers.

2.1 Non-Blind Spoofing

In this type of spoofing the attacker has straightforward access to the SNs and ANs. This type of attack takes place when attacker and the victim are part of the same subnet. The SN and AN can be sniffed, eliminating potential difficulty of calculating them accurately. This method is very easy and accurate for attack, but limited to connections going over your subnet. Various attacks that employ non-blind spoofing are discussed in Section 3.

2.2 Blind Spoofing

In this attack SNs are needed to be sampled by sending several packets to target machine. It is more sophisticated attack, because SNs and ANs are not reachable as attacker and target has no relationship what's so ever unlike in Non-Blind spoofing.

The reason such attacks succeeded was due to weak ISN selection which resulted in SNs that were simple to predict, thereby providing the attacker a window of opportunity. Over the years, this window of opportunity has slowly closed. However as many vendors eventually adopted stronger ISN selection methods. With nearly random SNs, an attacker might be required to generate billions of TCP packets in a very short time frame in order to successfully implement the attack [1][2].

3 ATTACKS EMPLOYING IP SPOOFING

IP spoofing is used as basis for number of other attacks on internet.

3.1 DoS Attack

A denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users from using the desired resources. Smurf, SYN, UDP and ICMP flooding are the most commonly used denial-of-service attacks [7].

3.2 Connection Termination

IP spoofing can be employed to terminate an ongoing communication session between two hosts. For this purpose the attacker uses TCP, RST and FIN packets.

3.3 Session Hijacking

Impersonating a legitimate host through a spoofed address and taking control of ongoing communication session. A DoS attack is launched against the spoofed host to prevent it from generating any replies while the attacker is communicating with the other host. The attacker forges the address and predicts the SYN/ACK numbers.

4 DEFENSES

Over the years number of solution to IP spoofing attacks have been proposed. But in one way or the other none of them provide efficiency, simplicity and full proof solution to such attacks.

4.1 Packet Filtering

Filtering techniques are implemented at the border routers of a private subnet to restrict address forgery. An access control list is implemented on the downstream interface of the border router that prevents the internal IP address range to appear as source address in incoming packets. This technique is referred to as Ingress packet filtering [6][1]. Similarly, implementation of an Access Control List (ACL) at the upstream interface of the router that blocks outgoing packets with source addresses other than the valid internal network range is called Egress packet filtering [6]. This prevents an internal host from spoofing the address of an external host.

4.2 Authentication

Authentication can be used to verify the identity of the sender by using various authentication methods such as HMAC, Kerberos, RADIUS, MD5, DIAMETER, TACACS etc. Digital certificates, digital signatures and some cryptographic algorithms such as Needham-Schroeder are also used for the authenticity. In IPv6, IPSec is mandatory that implements authentication using the Authentication Header (AH). Detail information is available in [8].

4.3 Encryption

To maintain the confidentiality of the data, the communicating pair can transform the transmitting data with encryption and decryption keys that are only known to the pair of hosts. IPSec implements Encapsulating Security Payload (ESP) that provides confidentiality through encryption at the network layer [8]. Link level encryption can also be employed against physical intrusions where each packet is encrypted as it leaves the host system. However it faces certain deficiency and deployment weaknesses [2].

5 PROPOSED SOLUTION

This is a novel solution that is both efficient and simple by which gateway routers on the destination network can detect and block spoofed packets. The solutions that are based on information currently found in the headers of TCP/IP packets are inadequate to protect network hosts against IP spoofing attacks [1]. Some additional information needs to be considered along with the source IP address for authentication. For this purpose we have included additional *Trusted Host ID (TID)* information that is unique to each user as show in (Fig 2) below. There were several potential candidate fields for the placement of TID in the IP header. These include the options field and the identification field. The options field was not selected as most routers do not process the IP options. Similarly most of the firewalls block the IP options. Moreover a fixed number of bits in the payload portion can also be allocated for the TID information. But the problem lies in the fact that the upper layer headers are encapsulated in the IP packet.

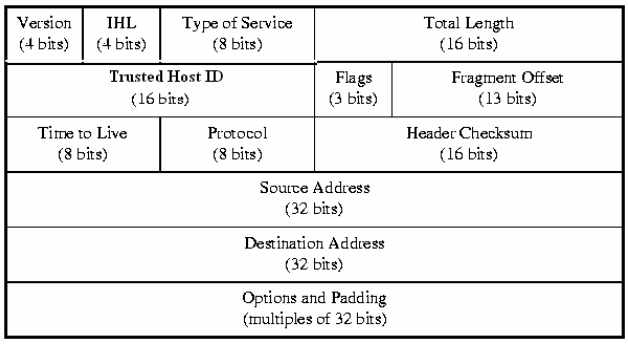

Fig.2. IP header with TID field

This could result in the overwriting of important upper layer header information. Therefore we have proposed that in our TID approach the information should be placed in the identification field. However the selection of this field also comes with certain issues. The basic problem is that it only works for packets that are not fragmented. However recent research has proved that most of the packets in the Internet are not fragmented [9]. The second problem lies with the size of the identification field. It is a 16-bit field therefore it only allows 2^{16} possible TIDs each of length 16 which are vulnerable to exhaustive search and brute force guessing. To overcome this we have embedded Trust Host Identification (THI) functionality.

5.1 Trusted Host Identification

The trusted host identification is calculated through the following steps:

1. The source address and the destination address are XORed to form an edge address.
2. A 16-bit hash is computed for the edge address.
3. Multiplicative inverse of the hash is calculated using Gallus Field (GF) (2^{16}) by a periodically changing primitive irreducible polynomial.

Since the edge routers observe all the outgoing traffic of the network therefore they are the best candidates to mark the packets. Each outgoing packet is marked with the TID by the egress router of the source network. At the destination network the ingress router is responsible for the processing and verification of the TID. The source and destination end routers periodically update each other on the primitive polynomial being used for each source-destination pair. If the TID computed on the destination ingress router does not correspond to the marked TID in the identification field of the packet, it is considered as spoofed and is discarded. If the TID is matched it is accepted as authenticated. This ensures that the source host lies within trusted source subnet.

The strength of this solution lies in the changing of the primitive irreducible polynomial. Moreover, since the computation of the TID is a complex function involving multiple operations therefore it is difficult to spoof.

6 CONCLUSION

IP spoofing is one of the major security concerns. It is the basic technique employed in most of the highly prevalent attacks. IP spoofing is difficult to prevent due the inherent security weaknesses in the current TCP/IP design specifications. Existing solutions include filtering techniques, encryption and authentication. We have suggested one potential

solution that involves modifications to the current IP header fields. Additional information about the host, referred to as the TID, is encoded in the identification field. This information provides a means to verify the authenticity of the source of the packet. Deployment of solution is suggested on the edge routers of the source and destination addresses.

7 FUTURE WORK

The major drawbacks of the proposed solution are spoofing attacks from within a same subnet. The routers shall not be able to distinguish between valid and spoofed packets. This will require some modifications in the router capabilities. Also this solution can be made computationally more viable. Some issues such as periodic changing and sharing of the irreducible polynomial needs to be addressed.

ACKNOWLEDGMENT

We would like to thank Mr. Imtiaz A. Khokhar and Miss Mehreen Afzal for various discussions and suggestions.

References:

[1] Nelson E.Hastings, Paul A. McLean, *TCP/IP Spoofing Fundamentals*, Computer and Communications, 1996.

[2] S. M. Bellovin, *Security Problems in TCP/IP Protocol Suite*, Computer Communication Review, Vol. 19, No. 2 1989, 32-48.

[3] Robert T. Morris, *A Weakness in the 4.2BSD Unix TCP/IP Software*, Bell Laboratory Technical Report, February 1985.

[4] Tsutomu Shimomura, Usenet Posting: *Technical Details of the attack of the attack described by Markoff in NYT*, January25, 1995.

[5] CERT Coordination Center, Cert Advisories: "CA-2000-01denial-of-service developments:" http://www.cert.org/advisories/ CA-2000-01.html; "CA-99- 17 denial-of-service tools," http://www. cert.org/advisories/CA-99- 1 7-denial-of-servicetools. html; "CA-98-1 3-tcp-denial-of-service: vulnerability in certain TCP/IP implementations," http://www.cert.org/advisories/ CA-98- 13-tcp-denial-of-service.1itml.

[6] P. Ferguson and D. Senie, "*RFC 2267: Network ingress filtering: defeating denial of s,ervice attacks which employ IP source address spoofing*," Jan. 1998.

[7] Daemon9, Infinity, and Routte, "*IP-spoofing demystified: trust relationship exploitation*," Phruck Mug., June 1996.

[8] Atkinson, R., "*Security Architecture for the Internet Protocol", RFC 1825*, August 1995.

[9] C. Shannon, D. Moore. and K Claffy. "*Characteristics of fragmented IP traffic on Internet links*", Internet Measurement Workshop, 2001.

[10] Angus Mackinnon et al., *Overview* of *Internet Protocol Security*, Technical Report 94-10, Monash University, Australia, October 27, 1994.