International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

A Novel Counter Measure to IP Spoofing Attacks

Kunal A

Department of Computer Application

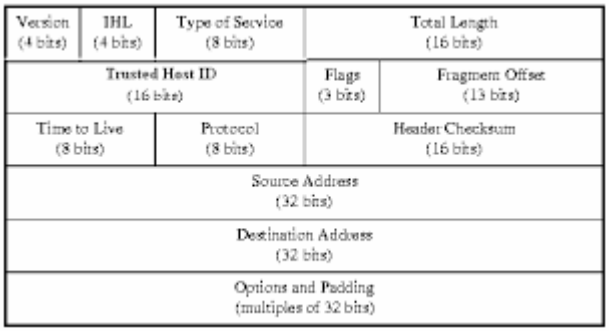
Dayananda Sagar College of Engineering

Abstract
IP spoofing is one of the most prevalent ways to hide your identity online. Hackers often use disguises to hide their true identity. TCP/IP protocol weaknesses are exploited to render it susceptible. TCP/IP protocol weaknesses may be exploited using methods such as beginning sequence number prediction and source address spoofing. Various IP spoofing risks and attack techniques are discussed in this article, along with various protective solutions such as router filtering and authentication.

Keywords: Spoofing, TCP, IP, Packet filtering, authentication, encryption, sequence prediction

1 Introduction

TCP/IP is the most frequently used protocol suite, since it is the most generally recognised. It explains how computers in a network communicate with each other. For ARPANET use in the 1970s, the Department of Defense built it. The TCP/IP family of protocols is used to perform a wide range of functions at various logical levels during communication. Link, Network, Transport, and Application are the four logical levels of a network. [1] Our concentration will be on the network and transportation levels. The network layer is used to allow hosts to interact with each other. Its primary functions are to handle information and data packets. TCP may be used to connect processes operating on different hosts. On the other side, there are a number of intrinsic security flaws. It was discovered that TCP/IP has flaws 2 and 3 throughout this examination. The network layer is where Internet Protocol (IP) is implemented. It includes useful information for the hosts' communication. Internet Protocol aims to send packets with the best possible effort (IP).



In the IP header, we're searching for the IP addresses of the source and destination (Fig.1.). It's important to keep an eye on things in these places. The contents of these fields may be changed by attack tools. Because machine IP addresses are not verified, an attacker might pretend to be the source of the assault [4]. Protocols like Transport Layer Protocol focus on establishing and maintaining network connections (TCP). A connection between the participating hosts is required before any data can be sent. A network connection cannot be established without a three-way handshake. The sender uses the SYN packet's first sequence number to formally request a connection (ISN). When the sender's ISN is acknowledged, a SYN packet is sent back to the recipient that includes the sender's ISN as well. Finally, the sender expresses gratitude to the receiver.

2 Spoofing Attacks

Spoofing is used by suspected hackers to mask their true identities. In general, hackers utilise one of two kinds of spoofing techniques.

2.1 Non-Blind Spoofing

This kind of spoofing attack gives the attacker direct access to the SNs and ANs. This kind of attack occurs when the attacker and the victim are both on the same subnet. The SN and AN can be sniffed, thus they don't need to be calculated precisely. This attack examines nonblind spoofing techniques, which are simple and accurate, but only operate on connections inside your own network.

2.2 Blind Spoofing

Many packets have to be delivered to the target computer to sample its SNs in this attack. Whereas with non-Blind spoofing the attacker and victim do not share any information. A vulnerability in the system's defences was exploited because of poor ISN selection, which led to predictable SNs. The chances of this occurring have lessened with time. Some organisations, on the other hand, started to implement more stringent criteria for selecting ISNs. [1][2] The attack leveraging nearly random SNs may need an attacker to create billions of TCP packets in a short period of time.

3 Attacks Employing IP Spoofing

Many internet-based assaults, such phishing and malware, use IP spoofing as their basis.

3.1 DoS Attack

A denial-of-service attack is used by an attacker to prevent legitimate users from accessing the targeted resources. Most often used denial of service techniques are Smurf, SYN, UDP, and ICMP floods.

3.2 Connection Termination

Interrupting a communication link between two hosts is possible with the use of IP spoofing. TCP, RST, and FIN packets are used by the attacker in this attack.

3.3 Session Hijacking

assuming the role of a legitimate host and seizing control of an ongoing communication session by using a fictitious IP address. A DoS attack is launched against the phoney host while the attacker is communicating with the other host. The attacker creates a fictitious address and knows just when to send the SYN/ACK numbers.

4 Defences

Countermeasures for IP spoofing attacks have proliferated throughout the years. However, none of them offers a response to such attacks that is efficient, simple, or totally secure.

4.1 Packet Filtering

Border routers on a private subnet may use filtering methods to prevent address spoofing. Access control lists are used on the border router's downstream interface to prevent packets from internal IP addresses. Ingress packet filtering is the term for this method. An Access Control List (ACL) at the router's upstream interface blocks outgoing packets with source addresses outside of the network's valid internal range when dealing with outbound traffic. If an internal host utilises an external host's address, the system will not be deceived.

4.2 Authentication

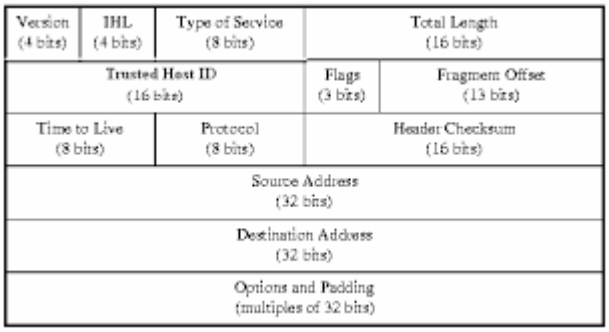
HMAC, Kerberos, RADIUS, MD5, DIAMETER, and TACACS are some of the authentication techniques you may use to verify the sender's identity. In order to authenticate digital certificates and digital signatures, Needham-Schroeder is employed. the authentication header must be used to verify the authenticity of packets in IPv6 (AH). [8] provides further information.

4.3 Encryption

Communications between two people may be protected by using encryption and decryption keys that only they know. IPsec's Encapsulating Security Payload (ESP) [8] provides network layer security. Physical intrusions may be prevented by encrypting each packet as it leaves the host system. A few limitations and flaws in its execution do exist [2].

5 Proposed Solution

Using this new, simple, and effective method, gateway routers on the destination network can detect and block forged packets. [1] IP spoofing attacks may be prevented by using TCP/IP packet header information, however this is not sufficient. There are many more pieces of information that must be taken into consideration throughout the authentication process. The extra Trusted Host ID (TID) information that we have supplied in (Fig 2) below is for this reason. The TID might have been inserted into a variety of IP header entries. The fields for selection and identification are two examples of this. Data in the top layer header might be altered as a result. As a result, we advised that the TID method integrate the information into its identifying field. Although this area has its advantages, it also has its disadvantages.



Only unfragmented packets may be handled by this method. Internet packets are not as fractured as was previously thought, according to new research. The size of the identification field is also a problem. Since there are only 216 possible TIDs of length 16, an exhaustive search and brute force guessing are pointless because of the field's limited length. The addition of THI capabilities is intended to alleviate this issue.

5.1 Trusted Host Identification

The following are the processes required to arrive at reliable host identification:

1. The source and destination addresses are XORed to produce the edge address.

2. The edge address generates a 16-bit hash.

3. By using an irreducible polynomial that varies often, the Gallus Field (GF) constructs the multiplicative inverse of the hash (216).

When a network's outward traffic is being monitored, packet labels should be applied at the network's edge router. The egress router generates a unique TID for each packet that leaves the source network. The TID is processed and verified by the ingress router of the destination network. Routers at the source and destination end of each source-destination pair share the same fundamental polynomial. If the destination ingress router's TID does not match the packet's identification, then the message is thrown out of the system. Authentication can only be performed if the TIDs are the same. They've shown themselves trustworthy.

6 Conclusion

Faking an IP address is one of the most common security threats. This core approach is the principal strategy used in the overwhelming majority of frequent assaults. The current TCP/IP design constraints have inherent security flaws that must be addressed in order to eliminate IP spoofing from the internet. All of the above are examples of current solutions, including filtering, encryption, and authentication. It's conceivable that IP header values may need to be tweaked as a workaround. The TID (Target Identifier) gives a unique identifier for each host. You may use

this information to check the packet's origin. Installing this repair requires access to the source and destination IP addresses' edge routers.

7 Future Work

It's not only spoofing assaults from inside the same subnet that represent a threat to the suggested technique. Fake packets can't be distinguished from real ones by routers. Because of this, we'll need to alter the router's capabilities. The computer's performance may also be improved. A number of issues must be handled, such as the periodic modification and sharing of an irreducible polynomial.

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-tcpdenial-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.