

# IP Spoofing: An Introduction

*Matthew Tanase* 2003-03-11

## IP Spoofing: An Introduction

by *Matthew Tanase*

last updated March 11, 2003

---

Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques. IP spoofing is one of the most common forms of on-line camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoofing" the IP address of that machine. In this article, we will examine the concepts of IP spoofing: why it is possible, how it works, what it is used for and how to defend against it.

### History

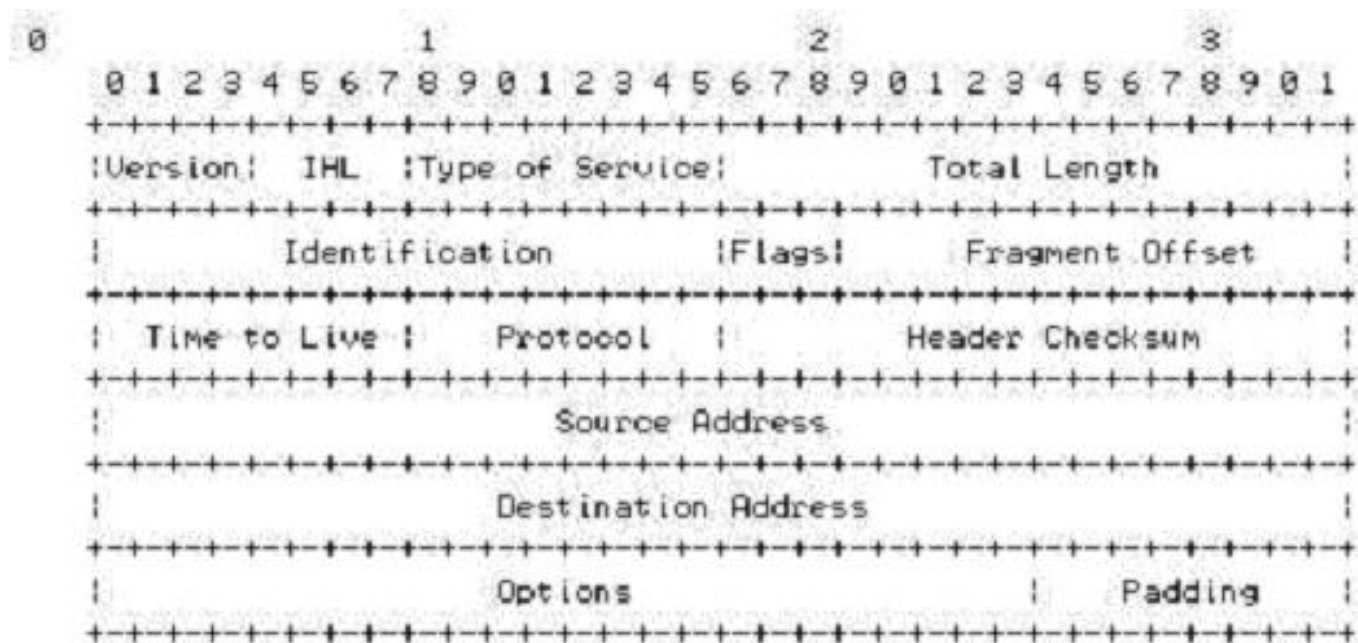
The concept of IP spoofing, was initially discussed in academic circles in the 1980's. While known about for sometime, it was primarily theoretical until Robert Morris, whose son wrote the [first Internet Worm](#), discovered a security weakness in the TCP protocol known as [sequence prediction](#). Stephen Bellovin discussed the problem in-depth in [Security Problems in the TCP/IP Protocol Suite](#), a paper that addressed design problems with the TCP/IP protocol suite. Another infamous attack, Kevin Mitnick's [Christmas Day](#) crack of Tsutomu Shimomura's machine, employed the IP spoofing and TCP sequence prediction techniques. While the popularity of such cracks has decreased due to the demise of the services they exploited, spoofing can still be used and needs to be addressed by all security administrators.

### Technical Discussion

To completely understand how these attacks can take place, one must examine the structure of the TCP/IP protocol suite. A basic understanding of these headers and network exchanges is crucial to the process.

### Internet Protocol – IP

[Internet protocol \(IP\)](#) is a network protocol operating at layer 3 (network) of the OSI model. It is a connectionless model, meaning there is no information regarding transaction state, which is used to route packets on a network. Additionally, there is no method in place to ensure that a packet is properly delivered to the destination.

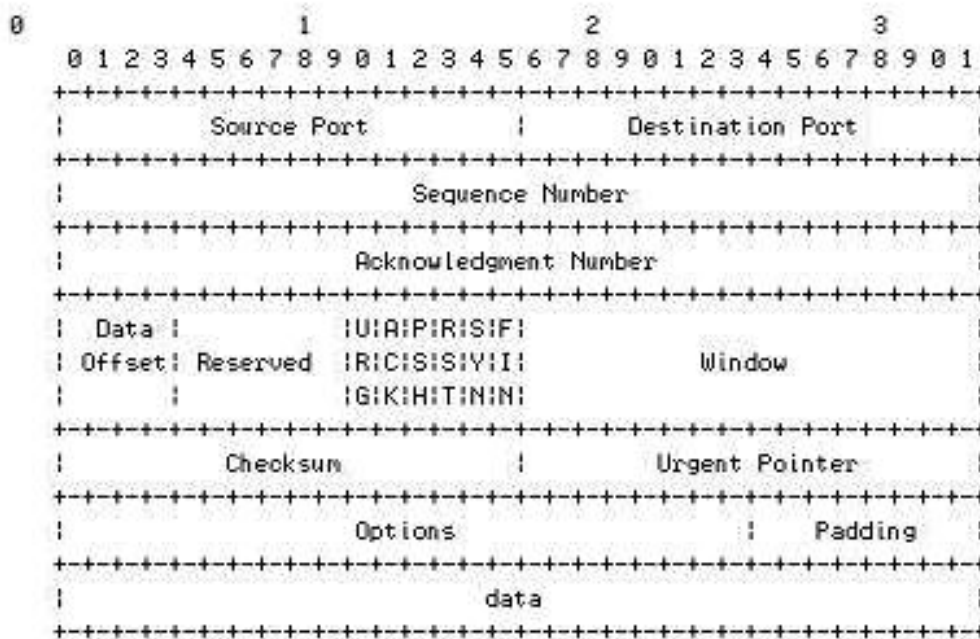


IP PACKET HEADER

Examining the IP header, we can see that the first 12 bytes (or the top 3 rows of the header) contain various information about the packet. The next 8 bytes (the next 2 rows), however, contains the source and destination IP addresses. Using one of several tools, an attacker can easily modify these addresses – specifically the “source address” field. It's important to note that each datagram is sent independent of all others due to the stateless nature of IP. Keep this fact in mind as we examine TCP in the next section.

## Transmission Control Protocol – TCP

IP can be thought of as a routing wrapper for layer 4 (transport), which contains the [Transmission Control Protocol \(TCP\)](#). Unlike IP, TCP uses a connection-oriented design. This means that the participants in a TCP session must first build a connection - via the 3-way handshake (SYN-SYN/ACK-ACK) - then update one another on progress - via sequences and acknowledgements. This “conversation”, ensures data reliability, since the sender receives an OK from the recipient after each packet exchange.



TCP PACKET HEADER

As you can see above, a TCP header is very different from an IP header. We are concerned with the first 12 bytes of the TCP packet, which contain port and sequencing information. Much like an IP datagram, TCP packets can be manipulated using software. The source and destination ports normally depend on the network application in use (for example, HTTP via port 80). What's important for our understanding of spoofing are the sequence and acknowledgement numbers. The data contained in these fields ensures packet delivery by determining whether or not a packet needs to be resent. The sequence number is the number of the first byte in the current packet, which is relevant to the data stream. The acknowledgement number, in turn, contains the value of the next expected sequence number in the stream. This relationship confirms, on both ends, that the proper packets were received. It's quite different than IP, since transaction state is closely monitored.

## Consequences of the TCP/IP Design

Now that we have an overview of the TCP/IP formats, let's examine the consequences. Obviously, it's very easy to mask a source address by manipulating an IP header. This technique is used for obvious reasons and is employed in several of the attacks discussed below. Another consequence, specific to TCP, is sequence number prediction, which can lead to [session hijacking](#) or host impersonating. This method builds on IP spoofing, since a session, albeit a false one, is built. We will examine the ramifications of this in the attacks discussed below.

## Spoofing Attacks

There are a few variations on the types of attacks that successfully employ IP spoofing. Although some are relatively dated, others are very pertinent to current security concerns.

### Non-Blind Spoofing

This type of attack takes place when the attacker is on the same [subnet](#) as the victim. The sequence and acknowledgement numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the datastream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection.

### Blind Spoofing

This is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable. In order to circumvent this, several packets are sent to the target machine in order to sample sequence numbers. While not the case today, machines in the past used basic techniques for generating sequence numbers. It was relatively easy to discover the exact formula by studying packets and TCP sessions. Today, most OSs implement random sequence number generation, making it difficult to predict them accurately. If, however, the sequence number was compromised, data could be sent to the target. Several years ago, many machines used host-based authentication services (i.e. Rlogin). A properly crafted attack could add the requisite data to a system (i.e. a new user account), blindly, enabling full access for the attacker who was impersonating a trusted host.

### Man In the Middle Attack

Both types of spoofing are forms of a common security violation known as a [man in the middle \(MITM\) attack](#). In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by "spoofing" the identity of the original sender,

who is presumably trusted by the recipient.

## Denial of Service Attack

IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against – denial of service attacks, or DoS. Since crackers are concerned only with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions. Rather, they wish to flood the victim with as many packets as possible in a short amount of time. In order to prolong the effectiveness of the attack, they spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block traffic.

## Misconceptions of IP Spoofing

While some of the attacks described above are a bit outdated, such as session hijacking for host-based authentication services, IP spoofing is still prevalent in network scanning and probes, as well as denial of service floods. However, the technique does not allow for anonymous Internet access, which is a common misconception for those unfamiliar with the practice. Any sort of spoofing beyond simple floods is relatively advanced and used in very specific instances such as evasion and connection hijacking.

## Defending Against Spoofing

There are a few precautions that can be taken to limit IP spoofing risks on your network, such as:

**Filtering at the Router** - Implementing [ingress and egress filtering](#) on your border routers is a great place to start your spoofing defense. You will need to implement an ACL (access control list) that blocks private IP addresses on your downstream interface. Additionally, this interface should not accept addresses with your internal range as the source, as this is a common spoofing technique used to circumvent firewalls. On the upstream interface, you should restrict source addresses outside of your valid range, which will prevent someone on your network from sending spoofed traffic to the Internet.

**Encryption and Authentication** - Implementing encryption and authentication will also reduce spoofing threats. Both of these features are included in [Ipv6](#), which will eliminate

current spoofing threats. Additionally, you should eliminate all host-based authentication measures, which are sometimes common for machines on the same subnet. Ensure that the proper authentication measures are in place and carried out over a secure (encrypted) channel.

## Conclusion

IP Spoofing is a problem without an easy solution, since it's inherent to the design of the TCP/IP suite. Understanding how and why spoofing attacks are used, combined with a few simple prevention methods, can help protect your network from these malicious cloaking and cracking techniques.

*[Matt Tanase](#) is President of [Qaddisin](#). He and his company provide nationwide security consulting services. Additionally, he produces [The Security Blog](#), a daily weblog dedicated to network security.*

## Relevant Links

[Session Hijacking Demonstration and Notes](#)

*Dave Dittrich*

[Closing the Floodgates: DDoS Mitigation Techniques](#)

*Matt Tanase, SecurityFocus*

[Privacy Statement](#)

Copyright 2006, SecurityFocus