

Journal Scientific and Applied Research, Vol. 31, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

AN OVERVIEW OF NETWORK ADDRESS AND PROTOCOL MESSAGE SPOOFING ATTACKS

Dimitar R. Iliev

Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: dimitar25_8000@abv.bg

Abstract: *Network protocols use addresses and control messages to exchange data and establish communication between devices. When this information is not properly verified, attackers can replace it with false information. This paper presents an overview of IP spoofing, MAC spoofing, NDP spoofing, and DNS spoofing. It explains how these attacks work, what conditions they require, and how they can affect network security. Their connection with man-in-the-middle attacks is also discussed. The paper compares basic protective measures, including source address filtering, port security, protection of IPv6 discovery messages, DNSSEC, and encrypted communication with proper authentication. The review shows why different spoofing attacks require different protection measures and why network addresses alone should not be treated as proof of identity.*

Key words: *Network security, IP spoofing, MAC spoofing, NDP spoofing, DNS spoofing, Man-in-the-middle.*

1. Introduction

Communication between network devices is very dependenr on the information carried in data packets and protocol messages. Devices use this information to identify destinations, discover neighbouring hosts, and find the IP addresses associated with domain names. However, it is possible for this information to be changed or forged. Spoofing is a technique in which an attacker provides false information to devices and makes traffic or protocol messages appear legitimate, when they are not. The attacker may imitate another device, redirect communication, or cause a service disruption. The result depends on the type of information being changed and the security controls used in the network. This paper reviews four types of spoofing: IP spoofing, MAC spoofing, NDP spoofing, and DNS spoofing. It describes their main features, possible effects, and the required protective measures. It also explains how these techniques may contribute to man-in-the-middle (MITM) attacks. It provides a descriptive comparison.

2. IP Spoofing

IP spoofing involves changing the source IP address in a packet. As a result, the packet appears to come from a different device. The attacker may use the address of a trusted host, the address of a victim, or another false address. This technique can be used in reflection attacks. The attacker sends a request to a service, in order for that service to reply and places the victim's IP address in the source field. The service then sends its response to the victim instead of the attacker. If the response is larger than the request, the attack can also amplify the traffic directed at the victim. Source address filtering can reduce this problem by rejecting packets whose source addresses do not match the network from which they came [1]. IP spoofing may also affect access controls that rely only on the source IP address. However, it does not automatically bypass all firewall rules or allow the attacker to receive the replies. A false source address alone is not enough to establish an authenticated connection or intercept communication. IP spoofing should also be distinguished from VPN use. A VPN carries traffic through a tunnel, and an external service may see the address of the VPN gateway. The main distinction is how the technologies work. The principle of IP spoofing is illustrated in Fig. 1.

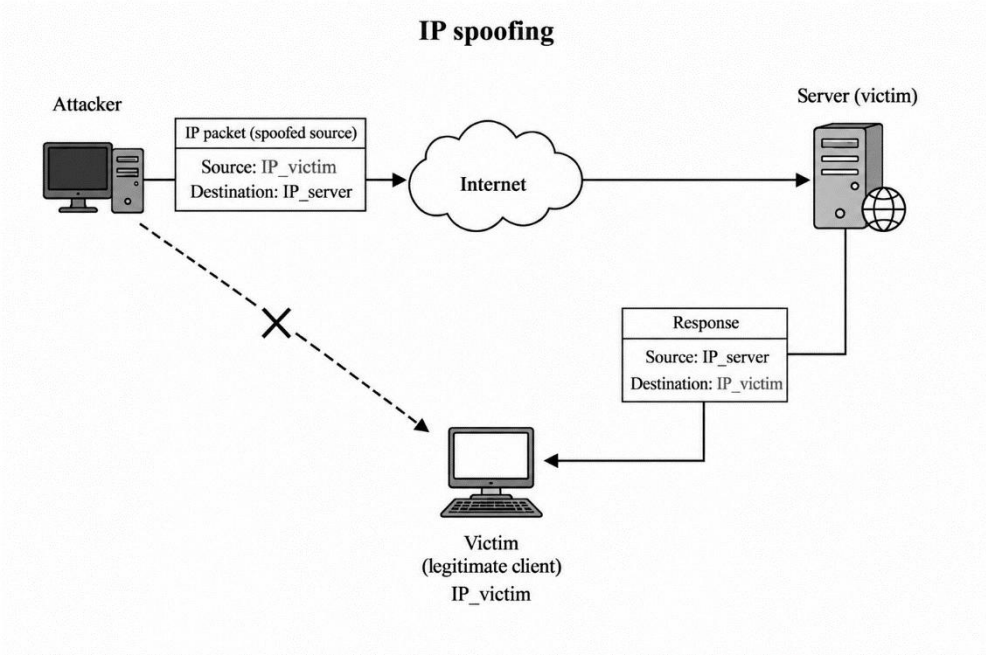


Fig. 1. IP Spoofing

3. MAC Spoofing

MAC spoofing involves using a different source MAC address in Ethernet frames. An attacker may copy the address of a legitimate device and attempt to appear as if that device is within the local network. Switches learn MAC addresses from incoming frames and associate them with switch ports. If frames containing a copied address arrive through another port, the switch may update its address table. Depending on the network configuration, this can cause incorrect frame forwarding, unstable connectivity, or device impersonation. These effects concern communication at the link layer. They should not be described as changes to IP routing. MAC spoofing also does not automatically allow the attacker to read all traffic in the network. Port security can help by restricting the source MAC addresses accepted on a port. However, a MAC address does not provide strong proof of a device's identity. For this reason, MAC-based restrictions should be combined with other ways of access control [2].

4. NDP Spoofing

The Neighbor Discovery Protocol is used in IPv6 networks to discover neighbouring devices and routers. NDP spoofing occurs when an attacker sends false discovery messages for another device to accept. For example, an attacker may claim that another host's IPv6 address is associated with the attacker's MAC address. If the receiving device accepts this information, it may send traffic to the attacker. False router advertisements can also influence which router a host uses. These actions can lead to traffic interception or Denial of Service [3]. One protective measure is Router Advertisement Guard, which restricts router advertisements received through unauthorized ports. However, this feature applies to router advertisements and does not protect against every type of NDP spoofing. Its effectiveness also depends on correct implementation, including the handling of IPv6 extension headers and fragmentation [4], [5].

5. DNS Spoofing

DNS spoofing involves providing false DNS information to a client or resolver. The aim is often to associate a legitimate domain name with an incorrect IP address. The client may then attempt to connect to a server controlled by the attacker. When the false information is stored in a DNS cache and reused, the attack is known as DNS cache poisoning. This can affect further requests that rely on the cached information. Checking whether a response matches an outstanding query and making query parameters harder to predict can reduce the chance of accepting a forged answer. These measures are discussed in RFC 5452 [6]. DNSSEC provides a way to verify the origin and integrity of signed DNS data. Its protection depends on successful validation through a trusted chain. DNSSEC does not encrypt DNS traffic or verify the content provided by the destination server [7]. DNS spoofing does not automatically defeat HTTPS. If the client correctly checks the server certificate for the intended hostname, a false server without valid credentials will be rejected. However, the redirection may still prevent the user from reaching the legitimate service [8].

6. Man-in-the-Middle Attacks

In a MITM attack, the attacker becomes an intermediary between two communicating parties. The attacker relays their traffic and may try to read or change the exchanged information.

Spoofing can help create the conditions for this attack. For example, false neighbour information may redirect local traffic through an attacker's device. A forged DNS response may direct a client toward an unintended server. However, not every spoofing attack results in MITM. Changing a source IP address alone does not give the attacker control over both directions of communication. The level of protection also matters. If the communication is not secured, the attacker may obtain sensitive information or modify messages. Properly authenticated TLS protects against reading and changing application data, even when the network path is not trusted. An attacker may still interrupt traffic, so encryption does not prevent every form of service disruption [8]. The principle of a man-in-the-middle attack is illustrated in Fig. 2.

The comparison shows why a single security measure cannot address all these attacks. Source address filtering does not validate DNS records, and port security does not authenticate a remote server. Each control addresses a specific part of the communication process. Network protection should therefore combine protocol-specific checks with application authentication. Monitoring changes in address mappings, router information, and DNS responses can also help administrators identify suspicious behaviour. Such changes require investigation, since they may also occur during normal network operation.

Probability of a Successful Attack

For attack type i, let O_i mean that the attacker has the access or opportunity required, A_i that the target accepts the forged information, and H_i that the selected harmful outcome occurs after acceptance. The probability that this attack path produces the harmful outcome is (1):

$$p_i = P(O_i) \times P(A_i \mid O_i) \times P(H_i \mid A_i, O_i) \quad (1)$$

Using shorter notation, equation (2) is obtained:

$$p_i = o_i \times a_i \times h_i \quad (2)$$

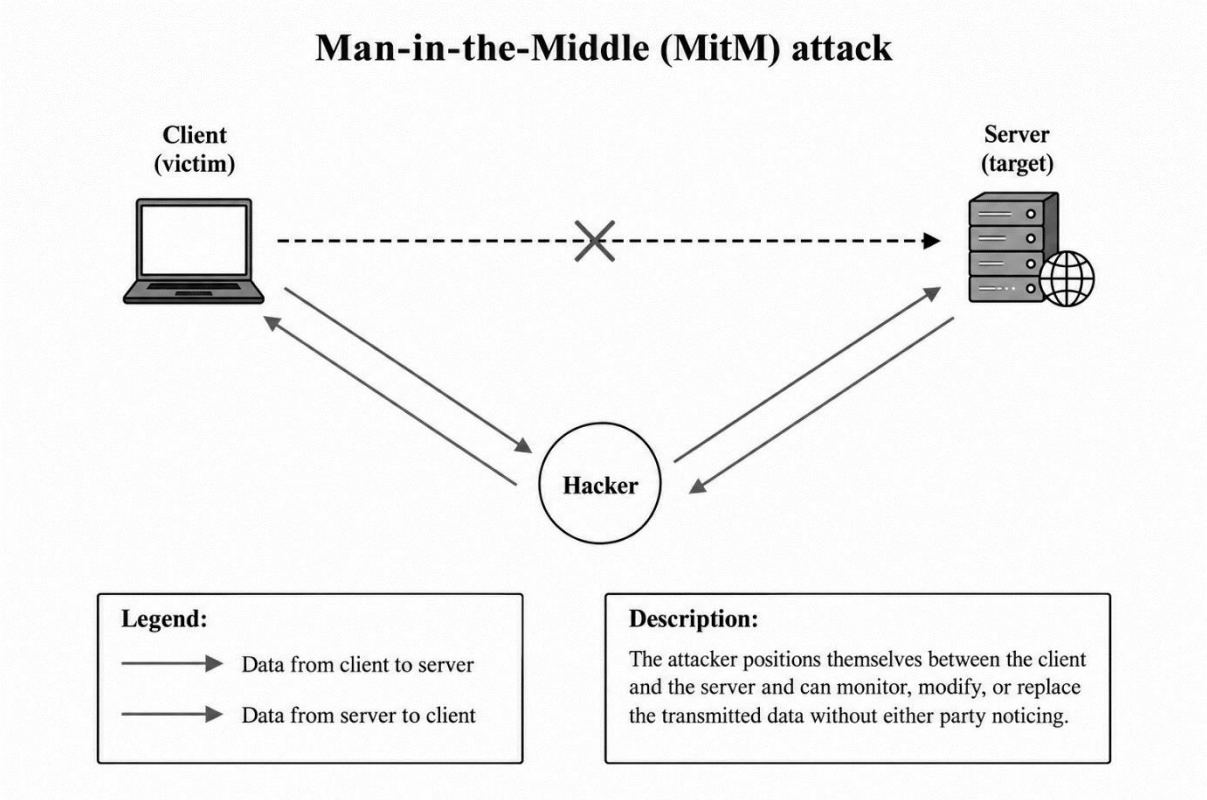


Fig. 2. "Man-in-the-Middle" Attack

7. Comparison and Protective Measures

The reviewed attacks affect different parts of network communication. Table 1 summarises their main differences.

Table 1. Main features of the reviewed spoofing attacks

Attack	Changed information	Possible consequences	Protective measures
IP spoofing	Source IP address	False attribution, reflection, Denial of Service	Source address validation and filtering
MAC spoofing	Source MAC address	Device impersonation, incorrect frame forwarding, connection disruption	Port security and network access controls

Attack	Changed information	Possible consequences	Protective measures
NDP spoofing	IPv6 neighbor or router information	Traffic redirection, interception, Denial of Service	Validation and filtering of discovery messages, check of router advertisements
DNS spoofing	DNS response information	Redirection to an incorrect server, cache poisoning	DNS response checks and DNSSEC validation

Here, o_i is the probability of having the required opportunity, a_i is the conditional probability of acceptance, and h_i is the conditional probability of harm after acceptance. Equation (1) follows the probability chain rule and does not assume that the events are independent.

The harmful outcome must be defined clearly. Traffic redirection, disclosure of information, and service interruption are different outcomes and should be evaluated separately. For example, a false DNS answer may redirect a connection attempt without allowing the attacker to read protected application data.

If N_i attempts have the same harmful-outcome probability, the expected number of harmful outcomes is (3):

$$E[X_i] = N_i \times p_i \tag{3}$$

When the probability differs between attempts, the expectation is the sum of their individual probabilities. Independence is not required for this expectation, although dependence matters when assessing the uncertainty of the results.

8. Conclusion

Spoofing attacks use false addresses or protocol messages to mislead network devices. IP, MAC, NDP, and DNS spoofing work in different ways, but they can all contribute to impersonation, traffic redirection, or service disruption. It is important to distinguish between forging information, intercepting traffic, and reading protected data. A successful attempt to change an address or redirect a connection does not necessarily give the attacker access to the contents of the communication. Effective protection requires controls suited to the affected protocol. Source address filtering, port security, protection of IPv6 discovery messages, DNSSEC, and correct certificate validation have different roles. Using these measures together can reduce the opportunities for spoofing while preserving normal network communication.

References

[1] Ferguson, P., Senie, D., Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827, BCP 38, May 2000.

[2] Cisco Systems, Port Security. Security Configuration Guide, Cisco IOS XE Dublin 17.12.x, Catalyst 9500 Switches.

[3] Nikander, P., Kempf, J., Nordmark, E., IPv6 Neighbor Discovery (ND) Trust Models and Threats. RFC 3756, May 2004.

[4] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., Mohacsi, J., IPv6 Router Advertisement Guard. RFC 6105, February 2011.

[5] Gont, F., Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard). RFC 7113, February 2014.

[6] Hubert, van Mook, R., Measures for Making DNS More Resilient against Forged Answers. RFC 5452, January 2009.
[7] Arends, R., Austein, R., Larson, M., Massey, D., Rose, S., DNS Security Introduction and Requirements. RFC 4033, March 2005.
[8] Rescorla, E., The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.