www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 3 Issue 4 April, 2014 Page No. 5540-5548*

# Network Security: Spoofing-The Online Attacks

***Mr. Vinod Saroha, Ritu Mehta, Sonia,Asha***
*Computer Science and Engineering*
*(Network Security)*
*Email-mehta.ritu27@gmail.com*
*B.P.S M.V.,Khanpur kalan Haryana*
*India*

***Abstract-***The main objective of this paper is to aware the computer users or other novice users about spoofing attacks. Spoofing means pretending something you are not, it is done in order to gain unauthorized access It is mainly the kind of attack that may harm the users in one or many ways depending upon the type of attack, during the spoofed attack attacker not only see our private information like password, user name, account number we type but also modify that precious information. There may be various types of spoofing attacks like web spoofing, URL spoofing ,e-mail spoofing ,IP spoofing etc here we describe the various type of spoofing attack &some useful method for prevent those internet attacks.

Keywords- Phishing, web spoofing, online attacks, filtering, trust, false web etc.

## 1. Introduction

"Spoofing is the situation in which one person or program successfully masquerades as another by falsifying information and data and thereby gaining an illgimate advantage[1]."

Spoofing attacks are possible in the physical world as well as electronic one. The idea of online spoofing was originating in 1980s with the discovery of security hole in the TCP protocol. In the internet world spoofing there are various form of spoofing.Genarally spoofing means false representation of some information. The aim of spoofing is make fools to the users and gain unauthorized access to the user private information like password, account number etc.Some of outcomes of spoofing may lead to theft, vindication and other malicious goal. thus we can say that spoofing is the major secuirity problem in the online internet services.

In this paper we will describe three main types of spoofing attacks and discuss some useful tips to prevent them:

- Web Spoofing (Internet con game)
- IP Spoofing
- DNS Spoofing

### 1.1 Elements that are involved in spoofing:

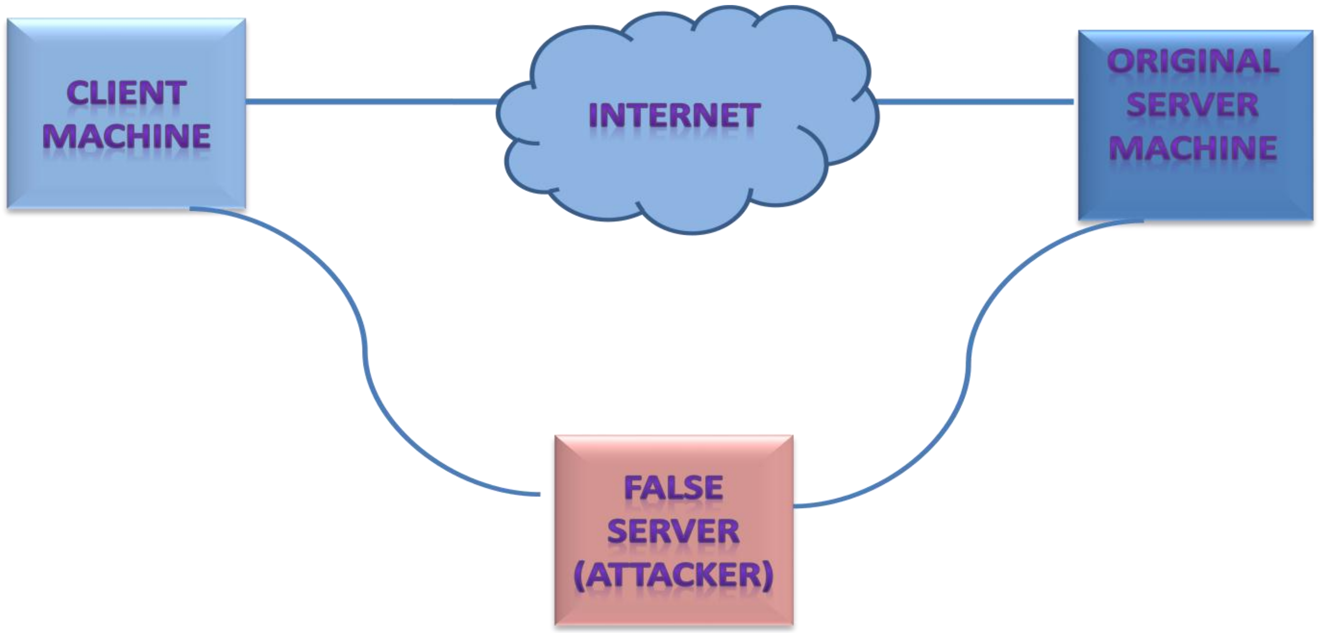


FIG 1:- Spoofing (man in middle attack)

- **Client machine:** Requests for service from original server machine.
- **Internet:** All transaction done over the internet
- **False server:** Before reaching to original server ,client requesting data are captured by attacker at his/her false server, now this captured data not only access by the attacker also it can be modified thus we can say that between original client and server middle man control the transaction and spoofed the original user and server i.e. known as man in middle attack.
- **Original server machine :** Original server is a real server to which client machine wants service but without the knowledge of client and server false server fools both.

## 2. Web Spoofing or Internet Con game

"It's a security attack that allows an adversary to observe and modify all web pages sent to the victim's machine and observe all information entered into forms by the victim."

Web spoofing is the internet con game in which attacker creates a mirror image of entire world wide web that look like a real one that have all links and web pages, through which process his/her transaction on the spoofing web site thinking as it is real and easily fools by the attacker.

The attacker uses the URL rewriting method to implement this attack. During this attack attacker sit between authorized user and rest of web.

.

## 2.1 Start the attack:

To start the attack the attacker put a rewritten link that goes to false web site on to the popular web page .Any user that wants a service from this web site directly click the link as is trusted web site link .but this is rewritten link provide by attacker to spoof the user.

User does request for the web service through their web browser like Firefox, internet explorer or Netscape navigator by clicking the link URL address e.g. www.ebay.com. Here the first part of URL "www" is host name and second part of the URL "ebay.com" is DNS (Domain name server).Our browser generally uses the second part of URL to determine the IP address of the host "www" in the domain "ebay.com". This above process is done by authorized user and he/she think as everything works smoothly.

But sometimes requested URL that we click link does not directly goes to that website instead it may go through the attacker server in the middle because this is the link provided by attacker that leads to the attacker server or false web server. To do this attacker change the URL and send back to the client. Let our actual URL is http://www.ebay.com and attacker rewrite it to "http://www.attacker.org/http://www.ebay.com" and user think as this http//attacker is the location of requested web server through which he/she wants service after clicking this link by user the attacker know the requested URL address through which client want to get their service and call the server for authorized user .Once the attacker fetch the real document to satisfy the request he/she can not only know the secret information like account number password etc of the user even change the requested information like amount, no. of item or any other information and get the service from original website. Now attacker server provides the rewritten web page to the client browser and client think that it comes from original server and follow the same link and spoofed continuously by attacker until leave that link.

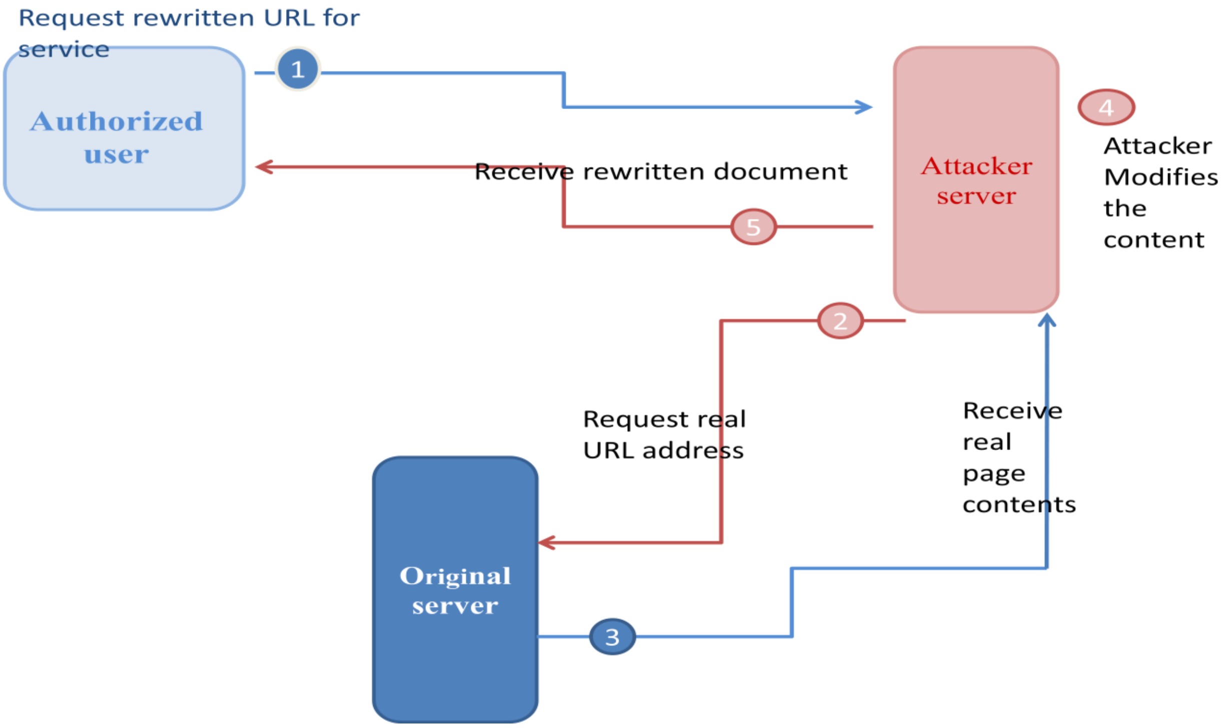

Request rewritten URL for service
1
Authorized user
Receive rewritten document
5
Attacker server
4
Attacker Modifies the content
2
Request real URL address
Receive real page contents
Original server
3

**FIG 2 :- Web spoofing**

### 2.2 Steps involved in Web spoofing:

1. **Request rewritten URL address for service**

   Rewritten URL is the spoofed address that look like the real URL that leads to the attacker website,this address is provided by the attacker for illegal

   access to the user account information and other data

2. **Request real URL address**

   As user request for spoofed address which leads to attacker server through which attacker receive the user information necessary for requesting the original server. Thus attacker request the real server for the service.

3. **Real page contents**

   Attacker receive the original page document from the original server **.**

4. **Attacker modifies the contents**

   As the attacker receives the real page document ,he/she can change the contents of page

5. **Receive rewritten document**

   Attacker server send the rewritten document or modified page content to the authorized user ,and he/she think that it comes from real server and easily spoofed by the attacker.

### 2.3 Useful tips for preventing the web spoofing attacks :

1. Pay attention to the web address of the website. A website look like a real one but it may be variation in spelling or use a different domain[2].
2. If you have any doubt about the site close it and contact directly to the company otherwise it may be dangerous for you.
3. Don’t click on the link given to popular social site, pop up windows or non trusted websites. These links may misguide you to different website than the expected one. Safe option is typing address in your browser[2].
4. Avoid using websites when the browser displays certificate or warning messages.
5. Only give sensitive information by verifying the web address begins with “https//” here ‘s’ indicate the secure connection rather than just “http//”.

## 3. IP Spoofing

“Replacing the true IP address of the sender with a different address is known as IP spoofing.”

IP spoofing is one of the most common form of on-line attacks. It is the process of using a fake IP address for communication with another machine, or for malicious purposes. Generally on the internet when we want to send any message, data or other content, these are broken into packets. Each packet header contains the source IP and destination IP address. When packet transfer from source to destination the receiving station read the source address so that it knows where the packet came from, and then send a reply to the machine at that address. But during “IP spoofing” attacker send message to the destination machine indicating that the message is coming from the trusted machine. To do this attacker first determine the IP address of the trusted machine then modifies the packet header field to that it appear as coming from trusted machine. After receiving the message destination machine will reply to that source address machine that it see in header field. Thus this service is mainly used when attacker do not care about response from the receiving machine or some way to guess the response.

IP spoofing is more frequently used in denial of service attack. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. Packets with spoofed addresses are thus suitable for such attacks. They have additional advantages for this purpose—they are more difficult to filter since each spoofed packet appears to come from a different address, and they hide the true source of the attack. This type of attack is most effective where trust relationships exist between machines like it is common on some corporate networks to have internal systems trust each other, so that users can log in without a username or password provided they are connecting from another machine on the internal network By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without an authentication.

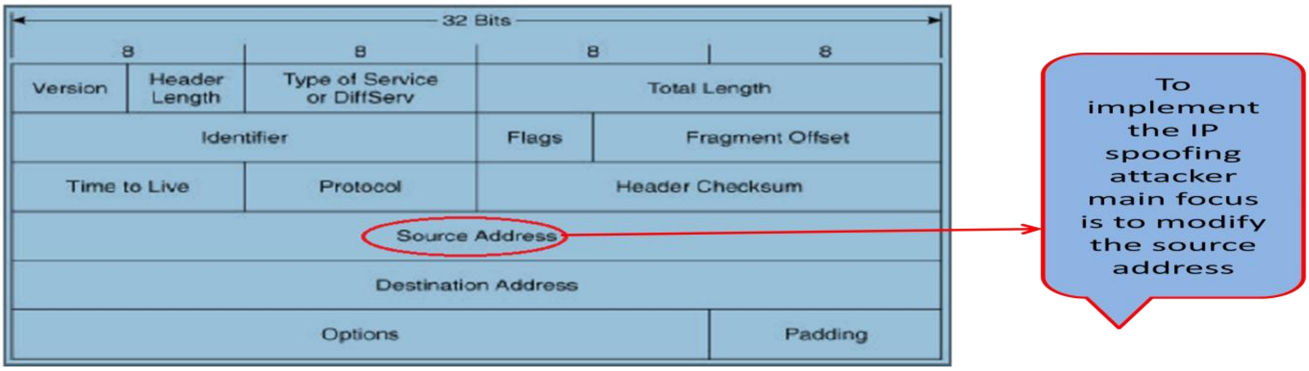


**FIG 3 :- Header of IP packet**

### 3.1 Steps for implementing the IP spoofing[3]:

1. Obtain a Target.
2. Obtain an IP address of the trusted machine.
3. Disable communication of the Trusted machine.(e.g. SYN flooding)
4. Sample a communication between the target and trusted hosts.
5. Guess the sequence numbers of the trusted machine.
6. Modify the packet header so that it appears that the packets are coming from the trusted host.
7. Attempt connection to an address authenticated service or port.
8. If successful attacker will plant some kind of backdoor access for future reference.

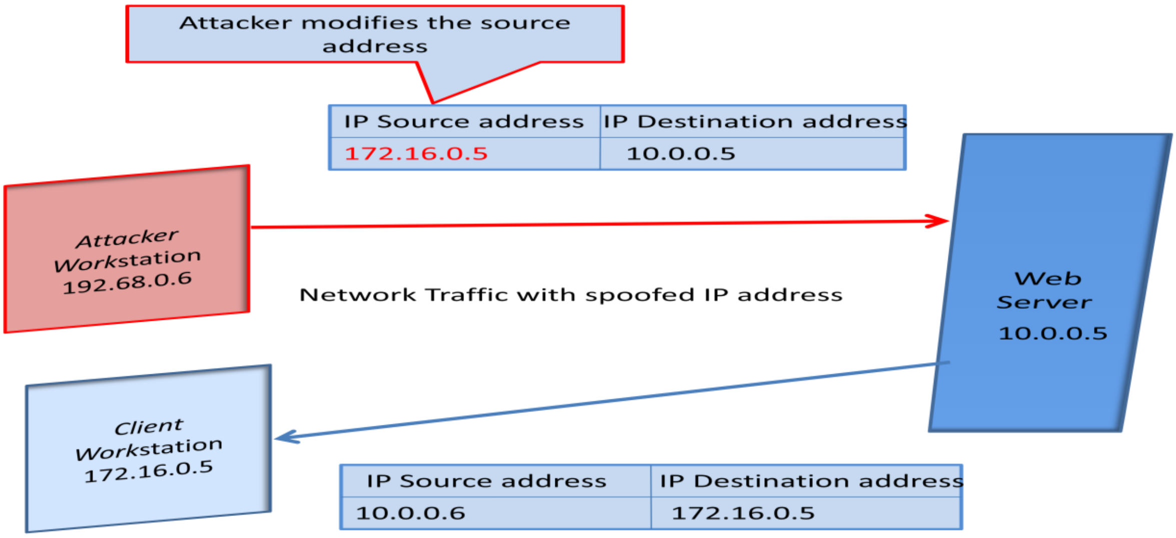

Attacker modifies the source address
IP Source address
IP Destination address
172.16.0.5
10.0.0.5
Attacker Workstation 192.68.0.6
Network Traffic with spoofed IP address
Web Server 10.0.0.5
Client Workstation 172.16.0.5
IP Source address
IP Destination address
10.0.0.6
172.16.0.5

**Fig 4:- IP spoofing**

### 3.2 Useful tips for preventing the web spoofing attacks[4]:-

1. Installing Input Filter: The best method for preventing the IP spoofing problem to install a filtering router that restricts the input to your external interface by not allowing the packet through it has a source address different from your internal network
2. Installing output Filter: Additionally we can install output filter in order to prevent a source IP spoofing attack originating from your site.
3. Use authentication based on key exchange between the machines on your network; Something like IPSec will significantly cut down on the risk of spoofing.
4. Use an access control list to deny private IP address on your downstream interface.
5. Enable encryption sessions on your router so that trusted hosts that are outside your network can securely communicate with you.

## 4. DNS Spoofing

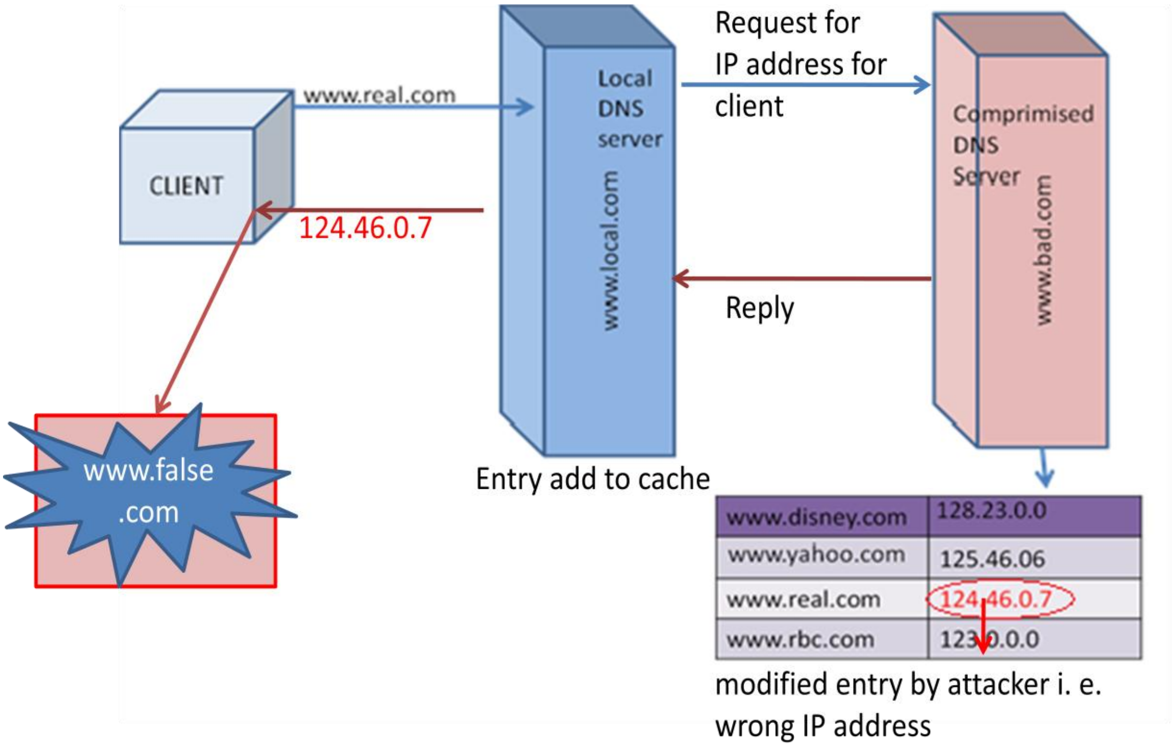
"When entry(for particular web site and its corresponding IP address) is not added correctly in the DNS server or any unauthorized user modified the DNS server entries is known as DNS spoofing.[5] "

DNS(Domain name system) is name system which has all the websites names and its corresponding IP address in its database in the form of records and placed in a hierarchical manner over internet. Generally when any user request for a particular website like www.gmail.com ,then the request for that particular web site IP address first going through the local server if that server find a entry for that that then it immediately reply the client otherwise local server send request to the top level DNS server in the hierarchy. In this way the DNS server resolve name resolution requests coming from the clients to the corresponding IP address thus client will able to access to particular web page.

When entry in the DNS server is modified in such a way that a particular website to an IP address that is not expected one then the client whose request is resolved by the DNS is redirected to the another web site that is not expected. This may create the problem for the client if he/she has to perform the necessary registration or transaction on that site this situation is DNS spoofing.

### 4.1 DNS spoofing technique:-

DNS spoofing is also known as **DNS cache poisoning** Method for implementing the DNS spoofing .Let there is a two server one which is Local DNS server with domain name www.local.com for your organization and the other is a comprimised DNS server with domain name www.bad.com. The attacker adds some customized entries, which includes legitimate website names with his own relevant IP address in the compromised DNS server. After that he sends a name resolution request for the IP address information of the domain www.bad.com to the DNS server of the domain www.local.com. Since the DNS server, does not have the information in its data base, it sends response to the attacker after getting the information from the comprimised DNS Server. During this transaction period, the DNS server of www.local.com not only receives the IP address information of www.bad.com but also the other records present in the DNS server in to its cache. This is normally referred to as cache poisoning. At this moment, if any client connects to local DNS server for name resolution he will be misguided to other website that is related to the attacker.



| | |
|---|---|
| www.disney.com | 128.23.0.0 |
| www.yahoo.com | 125.46.06 |
| www.real.com | 124.46.0.7 |
| www.rbc.com | 123.0.0.0 |

**Fig 5:- DNS cache poisoning**

One another technique for implement the DNS spoofing is **DNS ID spoofing**, when a name resolve request is generated by the client to send it to the DNS server, an ID will be generated along with the request. The client will accept the response for his request, if the ID of the response packet matches with the requested packet ID. But this way of name resolution is not secured. Because any unauthorized user can sniff the request and can create a response packet in the middle with the same id and IP address contained in it is not real ,it is the spoofed IP address to misdirect the client. This kind of DNS attack is known as DNS ID Spoofing

.

### 4.2 Useful tips for preventing the DNS spoofing attacks:-

1. Maintain the DNS software up to date.
2. Allow updates and zone transfers from trusted sources.
3. Maintain a Separate DNS server for public services and for internal services.
4. Use secure key for signing the updates received from other DNS server. This will avoid updates from entrusted sources

## 5. Conclusion

The paper describe an important internet security attack which is not difficult rather effective. Using the attack the attacker can observe and control everything the client do on internet. With the current implementations of spoofing, the network security community needs to be aware of the magnitude and potential cost of these types of attacks. People can effectively maintain patching and monitoring of logs to minimize the potential damage. Professionals must remain up to date with the Operating Systems and software that we use in our day to day activities. A steady stream of changes and new challenges is assured as the hacker community continues to seek out vulnerabilities and weaknesses in our systems and our networks.

## References

1. www.wikipedia.org/wiki/spoofing-attack
2. www.mountainone.com/socialengineering
3. Daemon, Route, Infinity, "IP Spoofing Demystified", Phrack Magazine;1996
4. www.searchsecuirity.techtarget.com
5. www.infosecawareness.in
6. www.google.in
7. R. Gross and A. Acquisti, "Information revelation and privacy in online social networks,"
8. http://www.fc.net/phrack/files/p48/p48-14.html;