IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IV (Sep – Oct. 2014), PP 111-115
www.iosrjournals.org

Teasers on Various Spoofing Attacks

Nikitha N[1], Maria krupa A[2], Rajeswari S[3]
[1](*Information Science department, New Horizon College of Engineering, India.)*
[2](*Information Science department, New Horizon College of Engineering, India.)*
[3](*Asst prof, Information Science department, New Horizon College of Engineering, India.)*

Abstract: *This paper proposed to give in depth survey on types of spoofing attacks. Spoofing is a way of masquerading identity of a person or a computer by providing fake data. In this paper huge variety of spoofing methods which includes brief introduction of Dns, Ip, Email, Arp, Web, Wireless, Mac spoofing. The intention of spoofing is to manipulate, steal data which in turn results in data loss and loss on millions of dollars.*
Keywords: *spoofing techniques, fake, attacker, network access, invader.*

I. Introduction

Spoofing is a type of deception where an intruder attempts to gain unauthorized access to a users system via pretending to be the user. Examples of spoofing are mitm, routing redirect, source routing, blind spoofing and flooding. Spoofing can have many forms in a computer world, all of which is a way of masquerading identity of a person or a computer by providing fake data. There are seven variety of spoofing attacks which are discussed below as,

- ARP (Address Resolution Protocol) Spoofing-Technique whereby an attacker sends fake ARP messages onto a LAN.
- WEB Spoofing-Activity that hackers use to direct website visitors to a website that looks like real one
- DNS (Domain Name System) Spoofing-It is one of the m-i-t-m attacks that force the victim to navigate to fake website purporting to be real one.
- IP (Internet Protocol) Spoofing-Hijacker obtains IP address of legal host and alters packet headers so that legal host appear to be the source.
- WIRELESS Spoofing-It is easy to launch and improves the performance.
- E-MAIL Spoofing-It is the creation of email messages with forged sender address.
- MAC (Medium Access Control) Spoofing-Technique for changing factory assigned MAC of a network interface on a networked device.

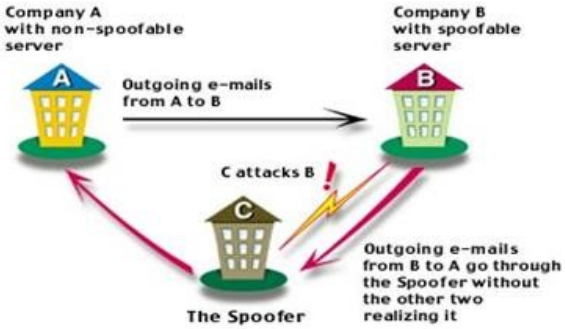

Fig 1.1 general spoofing

The above figure 1.1 shows how the attacker C intermediates between the company A and B and also tells that the email which is sent from B to A company goes through spoofer without the companies realizing it. The significance of these attacks can be very severe and can cost millions of dollars.

II. Survey On Types of Spoofing

2.1 ARP Spoofing

When TCP/IP over Ethernet became the most widely worn communication protocols. ARP (address resolution protocol) has no mechanism built to validate ARP packets, ARP spoofing is serious threat even today. To reach the objective of ARP spoofing, all the aggressor need to do is to send a fake ARP packet to the target host on the local area network. Once the target host gets the packets, it will update its ARP cache with new IP/MAC organization of corrupted data. This may result to the target host not able to communicate to the

proposed host or a man in the middle attack can expose the reliability of the packets. Because of the rapid development of wireless network, ARP spoofing, which used to exit only for LAN, has a new use field of attacking even for wireless network, which increases the difficulty on protection of ARP spoofing currently, the solution is through monitoring of the wireless network packets. [1]ARP protocol is based on mutually trust, it is a stateless protocol. The guarding algorithm for ARP spoofing is also one of the protective mechanisms against ARP spoofing [2]. Types of ARP spoofing are:

2.1.1 Sniffing: Here the attacker itself inserts between two communicating host to get the message, to prevent the halt the attacker retransmits the message.

2.1.2 Interception: It is based on sniffing. If the attacker C hides host A and sends the wrong message to host B to intermit link, the host A cannot communicate with host B the attacker send message to host A as host B to achieve interception goals .

2.2 WEB Spoofing

This is a kind of spoofing where the 'shadow copy' of the whole (World Wide Web) WWW can be created by an invader. It is like an electronic con game where invader forms a realistic but fake print of whole world web, the invader manages fake web thus all system transfer amid fatality browser and web will go through invader. Admission to the shadow web is directed through invader's device, permitting the invader to observe all the fatality's actions like his password. Ambiguous facts can also be sent to fatality as if it is from web server else to server as it's from fatality. thus invader can monitors and manages all the fatality does on the web. As the invader monitors and manages data of the fatality that has much potential as,

- Surveillance: Here even if fatality has a safer link(SSL) to server invader can observe, record all the details including confidential data of fatality as passwords, account number.
- Tampering: Here the invader not only record the details but also alters the fatality's data amid server and fatality.

Checking the spelling of URL, finding small hyphens and underscores and beware of java scripting are the steps to detect a spoofed web page. Signs of being a fatality are should click submit key recursively, enter password recursively, repainting to different web page and to check unanticipated mistakes. Thus web spoofing is risky and almost untraceable safety attack which is done on day today internet and the solution for fatality are of two types, they are short-term and long-term solution. Short-term solution consists of stopping JavaScript in your browser so that invader cannot conceal the proof of attack, location line should be seen forever and also to check URL on your browser location line whether it is directed to the correct server. Long-term solution consists of pages got through safer link better safer link pointer can help to get the pages [3]. The types of web spoofing are mentioned below,

- Dns server spoofing attack: Make changes of field name so that it directs to other IP address. It points again to other server hosting a spoofed site.
- Content theft: Replica of original site can be created by saving pages which are accessible publicly.
- Sub domain spoofing: Trapping the user as they are using right URL Make lengthy URL so that user does not read entire URL.

2.3 DNS Spoofing

This protocol is in application layer used to record individual legible area names to PC legible internet procedure (IP) address. it is important for internet operation.DNS usually work above the UDP (user datagram protocol) and UDP is chosen above the TCP (transmission control protocol).These are the 2 request for the comment which explains the rule for DNS execution.DNS spoofing attack goals at client's DNS resolver.DNS responses to the client are target UDP port, DNS operation ID and area name requested by client. Safety tools for DNS spoofing are paros proxy which will entrap the request and response to permit the data to be altered through communication procedure and Achilles proxy which is created for testing the safety of web applications. Here invader can Examine and alter client communication prior to send to the planned server.

The most capable DNS spoofing attacks for an outside invader are as follows, Glue attack, exploitation of chronological id, birthday attack. Cryptographic verification in the procedure is popular to make the outside attacks almost unfeasible. Cryptographic guard of DNS will tackle likely interior attacks like man-in-the-middle attack (MITM).MITM attack occurs when 2 parties are talking to each other. Here the invader is sandwiched between 2 parties. MITM goals at compromising the Confidentiality, integrity, availability. In Simulation copy of DNS spoofing attack, clients transmit packets to server and invader as a client disturb the computer and spoofs the injured DNS and packet is obtained.[4] Thus DNS is main part of internet communication, but it's weak to spoofing Based DDoS attack. Spoofed attack desire outcomes in DDoS attack by congesting a DNS server. The skill to guard from DDoS attack is spoof detection. Thus DNS guard is organized incrementally and clearly as fixed firewall. [5]

2.4 IP Spoofing

In day today internet, attackers fake the source address of IP packets equally to uphold their secrecy and forward the fault for attacks. When attackers insert packets amid spoofed source addresses hooked on the Internet, routers forward. Those packets go to their goal similar to other packet. Unluckily routers on Internet presently are not sorting spoofing packets efficiently. There are many solutions as Ingress/Egress filtering and Distributed Packet Filtering. Although solutions exist IP source address spoofing is a stern trouble on Internet. Attackers yet can spoof major part of current IP address. Thus we check and contrast diverse IP spoofing defence solutions in terms of three features as, mitigating spoofing attacks, Identifying spoofing packets, and pinpointing an attacker's real location**.** Spoofing defence solution can also be classified as shown below,

- End-Host-Based Solution: Here end host should identify spoofing packets. It will provide more security to a precise facility which includes active type and passive type.
- Router-Based Solutions: These prevent the spoofing packets yet to reach the end-host which includes basic filtering and distributed defence methods.
- Solutions Requiring the Use of Both Routers and End-Hosts: Routers and end-host should put effort mutually as these solutions should work. [6]

There is a HEMDADF (hashed encryption and marking based detection and filtering) scheme for protecting against IP spoofed attacks. It is of 3 parts: Marking process, filtering process, secure transmission. This scheme works even if 5000 attackers extremely attack spoofed packets. It detects incidence of attack by 4 seconds [7]. There is also a MDADF (marketing based detection and filtering) scheme for protecting against DDoS attacks. It is of 2 parts: marking process, filtering process. It also detects incidence of attack by 4 seconds so that suitable measures can be taken to reduce the harm caused by DDoS attack. [8]

2.5 WIRELESS Spoofing

As the wireless transmission means is open, invader can observe all the transmission. Later, the invaders can buy wireless machine which is of low cost and they use the usually existing stand to start different attacks with few attempt. Identity-based spoofing attack is one among types of attack which is easy to start and makes major harm to the network. Spoofing attacks provides different traffic injection attacks like attack on access control list, rogue access point attack, DoS attack. In major network, multiple opponents may cover-up as similar characteristic and team up to start mean attacks as network resource utilization attack and DoS attack. Thus to resolve such attacks must, spot the existence of spoofing attack, find out the number of invaders and focus many opponents and get rid of them[9].

The traditional method to find out spoofing attack is cryptographic authentication [10]. Appliance of cryptographic plan needs consistent key distribution, supervision and protection device. As the fear is on invaders who have various spot than legal wireless nodes, using spatial data to deal with spoofing attacks has the soul control to spot the existence of the attack and also to focus the opponents [9].Invader acts to the network as if they are another machine [10]. ROC (receiver operating characteristic) curve is a graph exactness of detection of attack versus fake positive rate. It's used to calculate attack detection plan. Spoofing attack detector after finding attack we must restrict the opponents and must get rid of invaders from the network. Thus we use real time localization scheme. We have a localization scheme and it is of 4 parts as mentioned below,

1) Transmitter: machine that forward packets can be focused.
2) Landmark: it's installed on each landmark with location known.
3) Server: centralized server gathers RSS data from all the landmark parts.
4) Solver: it takes input from server.

We included k-means spoofing detector into device to find out spot of an invader and also to get rid of the opponents from the network [9]. To find out the spot of an invader we used both point based and area based procedures in real time localization scheme [10].There are many solution models like,

2.5.1. GADE (generalized attack detection model): It is an attack revealing form which finds both spoofing attack and verifies number of opponents.

2.5.2. IDOL (integrated detection and localization): An integrated revealing and focusing scheme that finds out both attack and spot of many opponents even when the transmission control level is fluctuated. It will use the outcome of GADE to focus on many opponents. There are many IDOL methods such as,

- Generalized attack detection model: Have two stages which are attack detection, number determination.
- Determining the number of attackers: It's a multi class detection problem as we cannot correctly find out the number of opponents using similar characteristic.
- IDOL: It finds spoofing attacks, returns the number of invaders, focus the opponents.

Thus we use (received signal strength) RSS based spatial link, a material assets linked with each wireless gadget which is difficult to fake and does not depend on cryptography as source for finding out spoofing attacks in wireless networks [9].

2.6 EMAIL Spoofing

During email spoofing, an email message contains malevolent Objects and pretends to come from a valid source. But which is actually from an aggressor. Email spoofing is used for nasty purpose such as spreading viruses or other industrial spying activities Normal email has the return address at the top left corner .but the aggressors would have over written any address and name in this space which pretends to be true [11]. Spoofing is when an email comes from valid source but in reality comes from an aggressor. It is mainly for mal nasty purpose like spreading virus trawling for susceptible business data and other industrial activities. There is no guarantee that the letter is truly from that person and address .e-mail messages also contain return address but they can consciously misleading or "spoofed". Senders do this for different causes, including the following points,

- The email is spam and the sender doesn't want to be subjected to anti-spam laws
- The email constitutes a breach of some other law
- The e mail contains a virus and the sender believes we are more likely to open if it is from a know person
- The email request in sequence that we might want to give to the person the sender is pretending to be as a part of a "public engineering" molest.
- The sender is attempting to cause problem for somebody by pretending to be that person [12].

2.7 MAC Spoofing

Mac spoofing is a technique for changing a factory assigned Media access control (MAC) address of a network interface on a networked device. The MAC address is hard coded on the network interface controller and cannot be changed. They have discovered MAC Spoofing using only "air monitors", off-shells 801.11 devices are used to inactively sniff wireless traffic, without support from client stations [13].

2.8 URL Spoofing

It is a type of spoofing where a website seems as it's the other. The presented URL is not the actual URL of the spot. Thus the data is directed to concealed network address.Intrusion is a kind of URL attack where user is sent to a fake site by making the site to be alike in both appearance and texture of the original spot. Then the user tries to login with username and pin as the hacker gets the user's reserved data and then exhibits a pin error and leads the user to legal site. Now the hacker generates lot of bogus websites and takes off the secured data of the user without user knowing it. Web browsers issued safety covers (security patches) that will enhance the property of exposing the "exact" URL of a spot in the web browser. It is also necessary to confirm that the browser is exposed and should do the required updates. [14]

III. Conclusion

Today we find people from all the walks of life using internet regularly. On the other hand the problems and dangers in internet usage have also been increasing. There are many types of internet threats such as ID theft, virus attack, spoofing. Spoofing is the act of assuming the identity of some other computer. In this paper we discuss about Survey on types of spoofing and its pros and cons have been described above. Few methods have been mentioned in the paper which can be further used for implementation purpose.

References

[1]. jin-cherng Lin, men-jue Koo and cheng-sheng wang, A proposal for a schema for ARP spoofing protection Trans tech publication, Switzerland, 284-287, 2013.

[2]. Yangliu, kaikun dong, lan dong, and bin li,research of the ARP spoofing principle and a defensive algorithm, international journal of communication, vol.4, No.4,pp 516-520,2005.

[3]. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach,Web Spoofing: An Internet Con Game, Technical Report 540–96,1997.

[4]. Golriz Khazan and Mohammad Abdollahi Azgomi, DNS Spoofing Attack Simulation for Model-Based Security Evaluation, IJAST, vol.1,2010.

[5]. Fanglu Guo Jiawu Chen Tzi-cker Chiueh, Spoof Detection for Preventing DoS Attacks against DNS Servers proc of IEEE symposium,2012.

[6]. Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar, Controlling IP Spoofing Through Inter-Domain Packet Filters, dependable and secure computing,IEEE transaction, Vol 5,2006.

[7]. Vimal Upadhyay, Rajeev kumar, International Journal of Enterprise Computing and Business Systems, http://www.ijecbs.com, Vol. 1 Issue 2 July 2011.

[8]. Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El Saddik, and Amiya Nayak, Detecting and Preventing IP-spoofed Distributed DoS Attacks, International Journal of Network Security, Vol.7, No.1, PP.70–81, July 2008.

[9]. Deepa Hurali,Prof. Vidya R. Kulkarni,Detecting and localizing multiple spoofing attackers in wireless network, International Journal of Latest Trends in Engineering and Technology(IJLTET), 2013.

[10]. Yingying Chen, Wade Trappe and Richard P. Martin, Detecting and Localizing Wireless Spoofing Attacks, 4th annual IEEE communications society conference,2007.

[11]. Amala gracy and chinnapan jayakumar,identifying and locating multiple spoofing attackers using clustring in wireless network, international journal of wireless comunication and mobile computing,vol.1, no.4, pp 82-90, 2013.

[12]. P.ramesh babu, D.lalitha bhaskari and Ch.satyanarayana, A comprehensive analysis of spoofing, international journal of advanced computer science and applications, vol.1, no.6, 2010.
[13]. Yong Sheng, Keren Tan, Guanling Chen, David Kotz, Andrew Campbell, Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength, infocom 2008.27th conference on computer communications.IEEE, 2008.
[14]. Martina Sturdikova, Nekia Brice, Spoofing: The False Digital Identity, http://spoofing.njru.com/FinalPaper.html, cmpt 32, .may 2, 2007.