www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11301-11305

A Review on Media Access Control Spoofing

Srishti Gupta, Kirti, Jaya Chaudhary
CSE, SES, BPSMV
srishtig55@gmail.com
kirti.dahiya30@gmail.com
jaya.6aug@gmail.com

Abstract: This paper cover what is Spoofing, MAC spoofing; why people use it. This paper is a survey on MAC Spoofing. This paper have an overview of spoofing characterized , Vulnerabilities, working and operation , Detection of MAC Spoofing, Address Resolution Protocol. MAC spoofing. Mac spoofing is computer identity theft, for good or for bad reasons, and it is relatively easy. MAC spoofing has an address on a NIC (network interface card) ; it is inbuilt on NIC. A MAC Spoofing is to view the next-generation technology of IT industry. MAC Spoofing is applying to future spoofing servic

Keywords— MAC, STA, ARP

I. Introduction

What is Spoofiing?

• Spoofing is a process whereby one entity is a mask as another entity.

Why is spoofing done?

Spoofing A by B is done for various purposes

• B seeks the right of A

• B intends to hide its tracks

• As an attack on A

The ultimate goal of spoofing

• Unauthorized Service
• Get service on someone else's expense
• Loss of Service on Target
• Make sure that the target does not get any service
• Difficult to trace the attacker
• Make sure that people can not find who attacked them.
• Unnecessary packets clogging the network
• Make sure that nobody gets a good service.
• Secondary victim
• Primary target responds to spoof packet and overwhelm the source which becomes secondary victim.

Type of Spoofing

• MAC Spoofing

• IP Spoofing

• ARP Spoofing

• Control protocol internal header spoofing[7][8][10].

When a computer is connect to a Ethernet LAN it needs two addresses that is; the first is network card called MAC Address and second is IP Address. IP stand for Internet Protocol used by applications, independent of network technology operates under it. Each computer on a network must have a unique IP address for communication. IP addresses are virtual and are assigned through the software. MAC stand for Media Access Control. MAC address is an address of 48 bit. Each Network Interface Card (NIC) has a unique MAC address, it is inbuilt on it at the time of construction[5]. Exchange of MAC address over

the Local Area Network (LAN) identifies the two or more computer each other. MAC address is a Physical Address which is a permanentally allocated address. MAC address are necessary for Ethernet protocols for sending and receiving data, it is independent of application protocols. Ethernet make the frames and each frame has Ethernet header of size 24 bits and MAC address of size 48 bits for source and destination.

MAC address have two address fields inside it, one for Manufacture code and other for Serial Number[8].

MAC Adress	Manufacture Code	Serial Number
DD34.2344.13FD	DD34.23	44.13FD
110D.CC60.1388	110D.CC	6-.1388

II. Vulnerabilities of MAC Spoofing

1. **De-authentication:** The authentication protocol have message which is allows nodes to de-associate from each other in a single message. It call 6 re-authentication messages from a single de-authentication message. If this attack repeatedly occurs then victim could be kept from joining the network[2]. Various tools like Airjack [3], Void11 [4], can launch this attack easily.
2. **Power Saving Attack:** In this mode, the clients are in synchronous mode and the AP of all clients are in power-saving mode they wake up when receive the traffic indication map (TIM) and accept data from nodes. At this time an attacker can spoofs PS-Poll frame on behalf of a STA while it is in sleep or power saving mode. Then AP transmit the buffered frame continuously even when STA is not receiving frame as it was in sleep. Then attacker can block the victim STA from receiving frames from AP.
3. **Access Point Spoofing:** In this an attacker adds a fake AP with the MAC address and with SSID as a authorized AP in a public hotspot. Attacker should send the powerfull signal to steal the MAC address. Alternatively the attacker can implement as an active man-in-the-middle attack against HTTPS sessions by exploiting weak bindings in ad-hoc PKI [2]
4. **STA Spoofing:** An introduer spoofs the real STA, and gives the all access poits MAC addresses to the WLANs. And through thses access point addresses it can access other networks[5].

III. How To Spoof A MAC Address

Method 1:-

1. Click the Windows (Start) button and type cmd in the
search box. Hit Enter
2. In the black window that opens, type getmac /v then hit
Enter. It show MAC Address look something like XXXX-
XX-XX-XX-XX

1. Register your MAC address accordingly[4].

Method 2:-

1. Click the Windows (Start) button, select Run then type cmd then hit Enter.
2. In the black window that opens, type **ipconfig /all**. A page of information will scroll past including the Physical Address or MAC address.
3. Make the window larger then scroll back through the information to find your wired

and wireless MAC addresses will be labeled and will look something like XX-XX-XX-XX-XX-XX

4. Register your MAC address accordingly[10].

Method 3:

1. Click the Windows (Start) button, select *Run* then type **cmd** then hit Enter.
2. In the black window that opens, type **arp –a** then hit Enter. Your wired and wireless MAC Addresses will be appear with Internet Addresses, Physical Addresses and Type of Addresses will be present in that we will find IP Addresses, MAC Address and Type will be labeled and will look something like 192.172.21.1, XX-XX-XX-XXXX- XX and Static.
2. Register your MAC address accordingly[9].

Method 4:-

1. Open Network Connections,
2. Click on the specific wireless net icon.
3. Select Change settings for this network.
4. Look at the General tab, there is Dell TrueMobile 1150.
5. Choose Configure
6. Select the Advanced tab, and select the appropriate parameter
7. Fill in a new value[7].

Method 5:-

1. Navigate to the card configuration Windows dialog through Control Panel.
2. System, Hardware, Device Manager.
3. Right click the line for the card.
4. Choose Properties.
5. Input a new value[1]

IV. Detection of MAC Spoofing

Detection Methods: Detection methods can be classified as those requiring router support, active host-based methods, passive host based methods, and administrative methods. Administrative methods are the most commonly used methods today. When an attack is observed, security personnel at the attacked site contact the security personnel at the supposed attack site and ask for corroboration. This is extremely inefficient and generally fruitless. An automated method of determining the whether packets are likely to have been spoofed is clearly needed[3].

1. **Routing methods:** Because routers or IP level switches can know which IP addresses originate with which network interface, it is possible for them to identify packets that should not have been received by a specific interface. For example, a border router or gateway will know whether addresses are internal to the network or external. If the router receives IP packets with external IP addresses on an internal interface, or it receives IP packets with an internal IP address on an external interface, the packet source is most likely spoofed[11]

2. **Non-routing methods:** Computers who are receiving a packets can find if the packet is spoofed by a number of active and passive ways. Active means that the host must perform some network action to verify that the packet was sent from the claimed source. Passive methods require no need of these types of actions, however an active method may be used to validate cases where the passive method indicates the packet was spoofed.

   a. **Active Methods:** Active methods can do one of the two things either make queries to determine the true source of the packet (reactive), or affect protocol

specific commands for the sender to act upon (proactive). These methods have an advantage over routing methods in that they do not require cooperation between ISPs and can be effective even when the attacker is on the same subnet[10] as the target. Active methods require a response from the claimed source. Only if the spoofed host is active (i.e. connected to the network and receiving and processing packets) can it be probed. A host that is heavy firewalled and cannot respond to probes is effectively inactive[11].

b. **Passive Method:** Passive methods are a logical extension of the reactive methods.The data will have a predictable value, not relative to some prior packet, we can learn what values are to be expected and consider packets with unexpected values suspicious. Because TTL values are a function of a host's OS, the packet's protocol, and the network topology, all which are reasonably static, TTLs can be used as a basis for passive detection. Conversely, IP ID numbers, which generally have a strong relation to prior packets, do not make good candidates for the basis passive system[10][7][11][8].

Conclusion

In our paper we describe that MAC address will also be spoofed similarly as IP address spoofing. We have mentioned the various methods of spoofing the MAC address and various engines for its detection. The utility of detecting spoofed packets extends beyond simple detection .in our paper discuss about an attacker how can spoof the MAC Address. At a firewall to detect and block spoofed packets, the discussed techniques can be used to prevent spoofed packet attacks. If a MAC is spoofed its entry is made in registry, an opreting system (OS) may have the utility to check out its registry after few second if there is any entry with name network address then it should delete it therefore MAC cannot be spoofed.

References

1) **Basics:**http://ece.gmu.edu/~robohn/tcom509l2s03.pdfhttp://www.comptechdoc.org/independent/networking/guide/netarp.html
2) M.k.Choi1, R.J. Robles1, C.Hong, T.Kim1, Wireless Network Security: Vulnerabilities, Threats and Countermeasures, International ournal of Multimedia and Ubiquitous Engineering, Vol.3, No. 3, July, 2008
3) Y. Sheng, G. Chen, K. Tan, U. Deshpande, B. Vance, C. McDonald, H. Yin, T. Henderson, D. Kotz, A. Campbell, and J. Wright, "Securing 802.11 wireless networks through fine-grained measurements," Submitted to IEEE Wireless Communications Magazine.
4) R. A. Redner and H. F. Walker, "Mixture densities, maximum likelihood and the EM algorithm," *SIAM Review*, vol. 26, no. 2, pp. 195–239, 1984.
5) J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proceedings of the Twelfth USENIX Security Symposium*. Washington, DC, USA: USENIX Association, Aug. 2003, pp. 15–28.
6) A. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, D. S. Wallach, and G. Marceau, "Robotics-based location sensing using wireless ethernet," in *MobiCom '02:*

Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, Sept. 2002, pp. 227–238.

7) "MadWifi UserDocs: Antenna Diversity," technical document. [Online]. Available: http://madwifi.org/wiki/UserDocs/AntennaDiversity.