ISSN 2229-5518

Media Access Control Spoofing Techniques and its Counter Measures

Mrs. Hatkar Archana A, Ms. Varade Gauri A, Mr. Hatkar Arvind P

Abstract— The IEEE 802.3 MAC protocol is the standard for LAN Ethernet card in computer architecture. MAC addresses used for authorization by intrusion detection systems, can be spoofed to grant access to intruders on a wireless network. MAC spoofing is a means of changing the information in the headers of a packet to forge the source MAC address. By spoofing an address, the attacker can get packets through a firewall. A user may legitimately spoof the MAC address in order to reacquire connectivity after hardware failure. However, MAC address spoofing recently poses a serious security threat. In the past, several schemes have been proposed to leverage this problem. These previous methods incur high deployment costs in employing countermeasure protocols. This paper discusses different MAC spoofing techniques and its counter measures. We also emphasize on MAC spoofing techniques in Windows and Linux, spoof detection and its effectiveness.

Index Terms— Media Access Control, Network Interface Card, Ethernet Hardware Address, Address Resolution Protocol, Internet Protocol, Transmission Control Protocol.

---

1 INTRODUCTION

MEDIA Access Control address is a permanent address which is assigned to the network interface of every network connected device (NIC Cards, Wireless Adapters, etc) by the hardware manufacturers. Even though every network connected device has an IP address to identify them at the network layer (L3), the IP address is frequently changed .In contrast, MAC addresses are fixed and they function at the Data Link Layer (L2). A MAC address is also known as the physical address or the hardware address of a device. The changing of assigned MAC address may allow the bypassing of access control list on servers or routers, either hiding a computer on a network or allowing it to impersonate another network device. This is the spoofing of MAC address. Spoofing is used to impersonate a different machine from the one that actually sent the data. This can be done to avoid detection and/or to target the machine to which the spoofed address belongs.

This paper discusses the MAC Address, its representation, MAC Spoofing and its Counter measures. It includes detail techniques for MAC Spoofing in Windows And Linux, also sending packets via False IP, False MAC Address, False IP/MAC.

2 MAC ADDRESS NOTATION AND REPRESENTATION

2.1 MAC Notation

A MAC address, or Media Access Control address, is a 48-bit address (IPV4) or 64-bit address (IPV6) associated with a network adapter. While IP addresses are associated with software, MAC addresses are linked to the hardware of network adapters. For this reason, the MAC address is sometimes called the hardware address, the burned-in address (BIA), or the physical address. MAC addresses are expressed in hexadecimal notation in the following format: 01-23-45-67-89-AB, in the case of a 48-bit address, or 01-23-45-67-89-AB-CD-EF, in the case of a 64-bit address. Colons (:) are sometimes used instead of dashes (-).MAC addresses are often considered permanent, but in some circumstances, they can be changed. There are two types of MAC addresses:

1.Universally Administered Address:

The UAA, or Universally Administered Address, is the most commonly used type of MAC address. This address is assigned to the network adapter when it is manufactured. The first three octets define the manufacturer, while the second three octets vary and identify the individual adapter. All network adapter manufacturers have their own code, called the Organizationally Unique Identifier (OUI). For example, in the MAC address 00-14-22-01-23-45, the first three octets are 00-14-22. This is the OUI for Dell. Other common OUIs include 00-04-DC for Nortel, 00-40-96 for Cisco, and 00-30-BD for Belkin. Most large manufacturers of networking equipment have multiple OUIs.

2.Locally Administered Address:

The LAA, or Locally Administered Address, is an address that changes an adapter's MAC address. The LAA is a type of administered MAC address, and it is possible to change the LAA of a network adapter to any address of allowed length. When the LAA is set, the network adapter uses the LAA as its MAC address. Otherwise, the network adapter

- *Mrs. Hathar Archana A,Senior Lecturer in Department of E & TC Engg, SVIT, Nasik, India, Mobile No- 9420693529. E-mail:archana_hatkar@yahoo.co.in*
- *Ms. Varade Gauri A, Lecturer in Department of E & TC Engg, SVIT, Nasik, India, Mobile No- 9890923639. E-mail:varade_gauri@rediffmail.com*
- *Mr. Hathar Arvind P, Assistant Professor in Department of E & TC Engg, SVIT, Nasik, India, Mobile No- 9420693529.*

uses the UAA as its MAC address. All devices on the same subnet must have different MAC addresses, however. MAC addresses are very useful in diagnosing network issues, such as duplicate IP addresses, so it is a good practice to allow devices to use their UAAs instead of assigning LAAs, unless there is a compelling reason to do so.

MAC addresses are useful for security purposes, as they are only rarely changed from the default. IP addresses can change dynamically, especially on networks using DHCP to assign IP addresses, so MAC addresses are often a more reliable way to identify senders and receivers of network traffic. On wireless networks, MAC address filtering is a common security measure to prevent unwanted network access. In MAC address filtering, a wireless router is configured to accept traffic from certain MAC addresses. In this way, as white listed devices are assigned new IP addresses through DHCP, they retain their ability to communicate on the network. Any intruder attempting to impersonate a valid user on the network by masquerading with a faked IP address will not be able to do so because the computer's MAC address will not match any of those in the white list. This security method is only minimally successful, however, as a determined intruder can fake a MAC address almost as easily as an IP address.

2.2 MAC Representation

Numbering space managed by IEEE are in common use for formatting MAC address MAC-48, EUI-48 and EUI-64(Extended Unique Identifier). The original IEEE 802 MAC address comes from the original xerox Ethernet addressing scheme. The 48 bit address space contains potentially 248 or 281,474,976,710,656 possible MAC addresses.

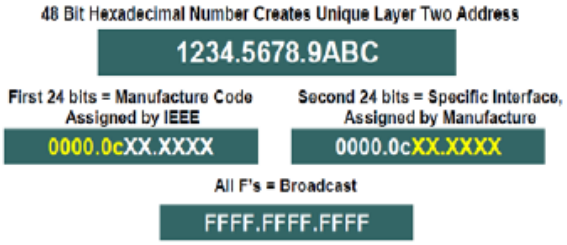

Fig. 1 Representation of MAC addresses

Fig. 1 shows the representation of MAC Address. Address can either be universally administered address or locally administered address. A universally administered address is uniquely assigned to a device by its manufacturer these are sometimes also called burned in address (BIA). The first three octets identify the organization that issued the identifier (OUI).

The remaining three octets are assigned by the organization in nearly any manner constraining the uniqueness. The locally administered address is assigned by network administrator that address do not contain OUIs. Universally administered and locally administered address are distinguishing by setting the second least significant bit of the most significant byte of the address. If the bit is 0 the address is universally admit if it is 1 the address is locally administered.

3 MAC Spoofing and its Techniques

3.1 MAC Spoofing

Although the physical MAC address are permanent by design and has world wide unique identification but there is a possibility to change the MAC address on most of the hardware. This action is basically referred to as MAC spoofing. This can be helpful for many reasons like when connecting to a WI-FI hotspot. Some internet service provider bind their services to a specific MAC address if users change their NIC the service won't work by changing the MAC address of the new interface will solve the problem. Some software licenses are bound to a specific MAC address. Changing the MAC address in this way is reverting to the MAC address physically stored in the card. But it is little different from IP address spoofing where a sender, which is sending something, spoofs its address as a request whereas in MAC the response is received by spoofing party.

Networking involves sending and receiving chunks of data between computers [2]. By splitting data into extremely small chunks called packets, we are able to share this data over greater distances in less time. When multiple computers are connected to a network, this data needs to know where it is going to and coming from in order to ensure that everything is delivered to the right place [3]. Each computer on a network typically has an Internet Protocol address (IP) and a MAC addresses (MAC). This information is added to the packet. When a packet comes to a computer, the computer opens the packet, reads the addresses and decides whether or not the packet is destined for that machine. This process is outlined in the networking OSI model which is beyond the scope of this fact sheet.

The problem is that it is possible for people to now change their computer's settings to replicate someone else's IP and MAC address. This can be done on a wired network; however, wireless networks are at a much greater risk because there is no physical connection needed and the attacker may connect from Published in International Journal of Advanced Engineering & Application, Jan. 2010 188 anywhere within the network's wireless radius. Also, there are a wide variety of wireless network cards that support the altering of MAC addresses. An attacker may pose as an authorized client or even "spoof" or "masquerade" as things such as wireless routers [4]. The problem here is that a user may connect to it thinking that this is the router their network is associated with and may unintentionally send personal information to it.

3.2 Vulnerability

A MAC address or Media Access Control, is the address hard coded into the Ethernet card. Changing it is possible.

Routers use these addresses along with IPs to route packets. In Some cases it is taken for good effect and in some cases for Bad effect, so some of the vulnerability are discussed below:-

1. By the use of a laptop, PC, personal data assistant (PDA) or hotspot locator (small electronic device that signals when it finds a wireless network in the area) an unauthorized user can find wireless networks simply by walking down the street. If the network found is secure, they may use MAC spoofing to gain access to this network depending on the level of security in use[9].
2. There are legitimate uses for MAC address "spoofing" for example; an Internet service provider (ISP) may register a client's MAC address for service and billing tracking. If the client needs to replace their network card, due to a failure or maybe a new computer, they can simply set the MAC address of the new card to that of the old one. Also, some software requires you to input your MAC address to access certain services. In this case, if the user needs to replace his/her network card, they may change their new network card MAC address to "spoof" their old one. This can eliminate the need to reregister the software product.
3. While it is possible to track illegal Internet traffic to a specific IP and to retrieve the name and address of the IP's registrant, it is very difficult to track which computer in a particular network engaged in the activity when the real offender is no longer connected to the network. MAC spoofing allows unauthorized access to someone else's network; therefore, responsibility for any illegal activity will fall on the authentic user. As a result, the real offender may go undetected by law enforcement.
4. MAC address is continuously being sent over Wi-Fi networks, even if they use secure WEP/WPA Encryption
5. Impact of MAC spoofing would be that approximately 50% of all traffic that should be delivered to the default gateway for routing will be delivered to targeted computer. The remaining client on the network will be unable to communicate with their default gateway.
6. Every new device on the network have its MAC address entered into the database as an authorized device. Therefore, if you can sniff the MAC address of an existing network node, it is possible to join the network using the MAC address of that node. Mac address filtering provides you effectively no protection against any hacker who has even an ounce of skill.
7. Once determined the target MAC address then tell the local attack box to switch its MAC address to that of the machine your wishing to duplicate (best to try duplicating a Domain Controller). Once Published in International Journal of Advanced Engineering & Application, Jan. 2010 191 switched our MAC address, an ARP request from the router or another host will embed our MAC/IP in the routing table of the switch. Because the switch now has two matching MAC addresses the internal processing of the switch will revert itself into a hub and broadcast the packets to the target and attackers box. Thus, one could sniff packets using Lophtcrack 2.5's SMB Capture utility[8].

It has been seen that switches are not port security enabled. It's up to engineers out to make sure that switches can only be accessed by a certain MAC address and a switch will not revert to a hub. There are drivers which allow to change the MAC address with different techniques in different Operating Systems.

Using CISCO CATALYST 6500 series switches which actually provide a group of spoofed MAC addresses for continuing the traffic forwarding without the knowledge of end station. When an active device fails it affects only the distributed performance and working speed but not the actual content of work. This technology could be used by an attacker to misuse the spoofed MAC address and attack the main server by the backend process (by using the same process but the attack is from the opposite receiving side to the main server).

3.3 MAC Spoofing Techniques And its Types

There are different MAC spoofing techniques. . In general, spoofing methods are used by crackers to compromise computer systems. Many people mistakenly think that spoofing is an actual attack. In reality, spoofing is just one step in a process whereby an attacker tries to exploit the relationship between two hosts. Two spoofing techniques are discussed with some guidelines on spoofing prevention.

Address Resolution Protocol Spoofing: The Address Resolution Protocol (ARP) provides a mechanism to resolve, or map, a known IP address to a MAC sublayer address.

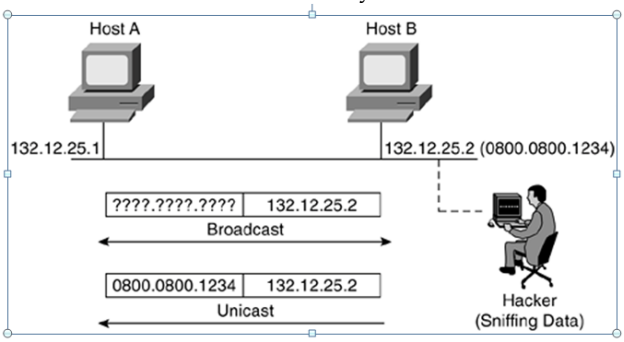

Fig 2. ARP Spoofing

Fig 2 ,two hosts are attempting to start a conversation across a multiaccess medium such as Ethernet. Host A wants to initiate the conversation with Host B but requires both the IP address and the MAC address. During the conversation setup, Host A is aware only of Hosts B's IP address, 132.12.25.2. To determine a destination MAC address for a datagram, the ARP cache table locally in Host A is checked first. If the MAC address is not in the table, Host A sends an ARP request, which is a broadcast on the wire looking for a destination station Host B with IP address 132.12.25.2. Every host on the network receives this broadcast. Host B hears the message, finds out the message is destined for it, and replies with an ARP reply containing its MAC address and IP address. There is no real authentication; the verification between two hosts is based only on the hardware address, which is a weak part of the ARP process. Using ARP spoofing, the cracker can exploit

this hardware address authentication mechanism by spoofing the hardware address of Host B. Basically, the attacker can convince any host or network device on the local network that the cracker's workstation is the host to be trusted. This is a common method used in a switched environment.

Domain Name Service Spoofing: Domain Name Service (DNS) is used for network clients who need an IP address of a remote system based on their names. The host sends a request to a DNS server including the remote system's name, and the DNS server responds with the corresponding IP address. DNS spoofing is the method whereby the hacker convinces the target machine that the system it wants to connect to is the machine of the cracker. The cracker modifies some records so that name entries of hosts correspond to the attacker's IP address. There have been instances in which the complete DNS server was compromised by an attack.

4 Counter Measures

Spoofing is a means to hide one's true identity on the network. To create a spoofed identity, an attacker uses a fake source address that does not represent the actual address of the packet. Spoofing may be used to hide the original source of an attack or to work around network access control lists (ACLs) that are in place to limit host access based on source address rules.

Although carefully crafted spoofed packets may never be tracked to the original sender, a combination of filtering rules prevents spoofed packets from originating from your network, allowing you to block obviously spoofed packets.

The generalized Countermeasures to prevent spoofing include:

- Filter incoming packets that appear to come from an internal IP address at your perimeter.
- Filter outgoing packets that appear to originate from an invalid local IP address.
- Counter measures to prevent threat of spoofing the user identity include:
- To use strong authentication.
- Not to store secrets in plaintext.
- Not to pass credentials in plaintext over the wire.
- To protect authentication cookies with Secure Sockets Layer (SSL).

Following are some more counter measures to prevent MAC spoofing:

1.Whenever ARP packets arrive it should not check the MAC Address for the OS, its should retrieve it directly from LAN card or when ever ARP packets arrive it should compare the MAC Address from OS to NIC and if it doesn't match it should delete the entry from OS or from registry.

2. MAC Address is stored in OS whenever MAC Address is required it is retrieve from Operating System if we want to prevent MAC Address to be spoofed then whenever we require MAC Address we must retrieve it directly from NIC.

3. You can lock your MAC Address by introducing the router which support the MAC filtering and IP Reservation. This is where you associate a DHCP IP address with a particular MAC address. This way only that MAC gets that particular IP address.

To prevent MAC spoofing you would need to encrypt the communication between the wireless pc and access point.

5 Conclusion

Spoofing is possible because the IEEE 802.11 standard does not provide per-frame source authentication [10], but in future it can be effectively prevented if a proper authentication is added into the standard. There is plan for such standard modification to support link-layer source authentication that covers both management and control frames. The key idea of this project is to leverage the sequence number field in the link-layer header of IEEE 802.11 frames without modifying STAs, APs, or the MAC protocol. If an intrusion detection system keeps track of the latest sequence number of each wireless node, to impersonate a node an attacker needs to spoof the source address as well as its corresponding sequence number. If the sequence number of a spoofed frame is equal to or smaller than the corresponding node's current sequence number, the spoofed frame is considered a retransmitted frame and thus has to have the same content as the authentic frame with the same sequence number. This means that the spoofed frame cannot possibly do any harm as it is just a duplicate. If a spoofed frame's sequence number is larger than the corresponding node's current sequence number, some subsequent authentic frame will have the same sequence number as this spoofed frame and eventually expose the spoofing. It designs and evaluates a detailed algorithm on sequence number-based spoofing detection. In real world tests, the false positive rate of the proposed algorithm is zero, and the false negative rate is close to zero. In the worst case, the proposed algorithm can detect a spoofing activity, even though it can only detect some but not all spoofed frames. Although several commercial systems claim that they can also detect spoof, the details and effectiveness of their detection mechanisms are largely unknown. MAC spoofing attacks in 802.3 networks exploit a fundamental vulnerability of the 802.3 protocols. The MAC addresses of the Ethernet LAN card can be easily forged, imposing a serious security challenge.

With this we conclude that the dangerous security hole is in our OS. Our OS is static but if it will be dynamic it will resolve our many spoofed based problem. If a MAC is spoofed its entry is made in registry, a dynamic OS may have the utility to check 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] D.C. Plummer, An Ethernet Address Resolution Protocol, RFC-826, Network Working Group, November 1982.

[2] C. Hornig, A Standard for the Transmission of IP Data grams over Ethernet Networks, Symbolic Cambridge Research Center, Network Working Group,

April 1984.
[3] T. Pusateri, IP Multicast over Token-Ring Local Area Networks, RFC-1469, Network Working Group, June 1993.
[4] M.D.Spivey, Practical Hacking techniques and countermeasures,
[5] SMAC: http://www.klcconsulting.net/smac
[6] http://www.snapfiles.com/php/download.php Packet
[7] VMware Workstation: http://www.vmware.com
[8] Y. Liu, K. Dong, L. Dong, B. Li, Research of the ARP Spoofing Principle and a Defensive Algorithm, International Journal of Communications.
[9] 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
[10] A.William A.Shankar, Narendar, Wan, Y.C. Justin.. your 802.11 wireless networks have no clothes. March 2001.
[11] http://en.wikipedia.org/wiki/ MAC spoofing