

Media Access Control (MAC)

MAC SPOOFING AND ITS COUNTERMEASURES

First A. Deepak Gupta¹, Second B. Gaurav Tiwari¹,
Third C. Yachin Kapoor² and Fourth D. Praveen Kumar³

¹Bhagwan Parshuram Institution of Technology, Delhi, India

Email: {myself.deepakgupta¹, gtiwari1988¹}@gmail.com

²COMMIT Career Academy, Delhi, India, ³Maharaja Agrasen Institute of Technology, Delhi, India

Email: {Yachin_2005², Praveen.mait³}.@yahoo.com

Abstract— When computers connect together on a network, a network card or wireless network card are typically used. Each network card or wireless network card has a Media Access Control (MAC) address that is used to tell them apart. The MAC address is a series of 12 characters usually in the form xx-xx-xx-xx-xx-xx and is burned into the hardware of a network card. The first 6 characters distinguish what company made the card and the rest are unique to identify that specific card. This is in accordance with IEEE (Institute of Electrical and Electronics Engineers 1) standards. MAC address spoofing refers to someone changing their MAC address in order to resemble that of another network card for various reasons.

This Specification defines the different MAC Spoofing Techniques and its Countermeasure. This document includes detail description about MAC Address, Representation of MAC Address, MAC Spoofing Technique in Windows and Linux, Need of MAC Spoofing in Ethical Security and Non Ethical Security, its Countermeasure and future scope.

Keywords - MAC, NIC, ARP, LAN, IP, OS.

I. INTRODUCTION

This Specification defines the MAC Address, its representation, MAC Spoofing and its Countermeasures. It includes detail techniques for MAC Spoofing in Windows And Linux, also sending packets Via False IP, False MAC Address, False IP/MAC i.e. PACKET.

The author will like to acknowledge the Contribution of the Keyword “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119].

II. MAC ADDRESS

Media Access Control Address is a permanent and world wide unique identification assigned to most network adapters or NICs i.e. Network interface card by the manufacturer and used in the Media Access Control

Protocol Sublayer. If MAC address is assigned by manufacturer, it usually encodes the manufacturer’s registered identification number which may also know as EHA i.e. Ethernet Address, Hardware Address, adapter address or Physical Address.

MAC Address is UNIQUE for all network machines then why we need IP?

Their hierarchies under which they are organized are useless for routing. Let your Ethernet card’s MAC Address is “Made by Semiconductor”. If a Machine Wanted to send you a packet would not know how to route that packet to your machine. IP Address are hierarchical by route so if remote machine send a packet to 192.168.1.2.its router can lookup a table that says “Send all 192.68.x.x packets to router doesn’t need to know who is responsible for that “block” of IP Address .It could do because IP Address are hierarchical by location .in the wiring plan whereas MAC Address are only hierarchical by manufacturer.

MAC Address Notations

Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits which specify the interface serial number for that interface vendor.

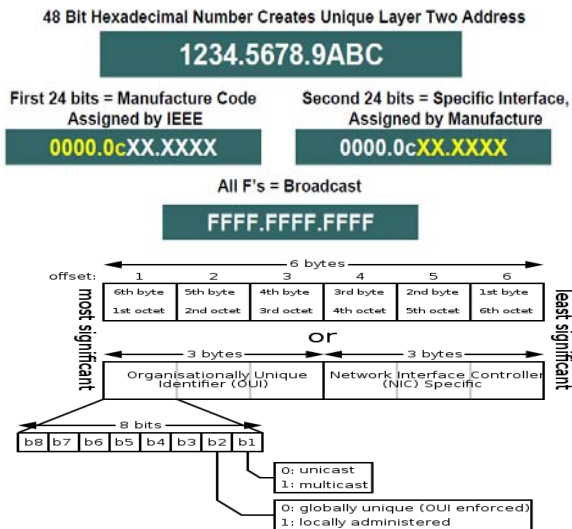
The Standard (IEEE 802) format for printing MAC-48 addresses in human-friendly form is six groups of two hexadecimal digits separated by hyphens (-) or colon (:) in transmission order e.g. 01-23-45-56-67-ab, 01-12-23-34-56-ab. This form is also commonly used for EUI-64. Other less common convention use three groups of four hexadecimal digits separated by dots (.) e.g. 0123.4567.89ab; again in transmission order.

MAC Address 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 2^{48} or 281,474,976,710,656 possible MAC address.

¹Yachin Kapoor, ²Gaurav Tiwari, ³Praveen Kumar are the student and ⁴Deepak Gupta, Lecturers of Bhagwan Parshuram Institute of Technology, New Delhi INDIA (phone: 2757-1080; fax: 2757-2224; e-mail: myself.deepakgupta@gmail.com).



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 following three octets are assigned by the organization in nearly any manner they please Subject to the constraint of uniqueness. The locally administered address is assigned by to a device by a networks administrator address do not contain OUI s. 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 of the address is locally administered.

Is it possible for a PC to loose its MAC address configuration permanently?

What I mean is, my PC crashed during a thunderstorm, after it came back on I could no longer access my network at home. Which is using DHCP and PC recognized the connection it to my LAN I was able to connect I also connected it directly into a device that is using DHCP and the PC recognized the connection. I then brought the PC home and reconnected it, in the hope that by some slim chance it would work, it did not. So that is why I am asking if it is possible for a PC to permanently loose a MAC address.

III. 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 bit different from IP address spoofing where a person which is sending something spoof its address in a request tricks the other party into sending elsewhere, in MAC the response is received by spoofing party.

Both parties cannot determine from the MAC address whether they are the same OSI Layer 2 Network.

Is it possible for a service provider to detect that a MAC address is being spoofed?

Service provider may guess For Example, for month I use x Kilobyte of bandwidth per month. I then make a request using another MAC address (my router) which fails. Soon after I revert back to my old MAC address (spoofed by the router). My bandwidth usage subsequently increases to 2x Kilobyte a month, one could guess that I now have two machine behind the router but this can not be proven by the service provider.

How does it Works?

Networking involves sending and receiving chunks of data between computers. 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. 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 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. 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.

MAC SPOOFING TECHNIQUES (A) IN WINDOWS

Method 1:

This is depending on the type of Network Interface Card (NIC) you have. If you have a card that doesn't support Clone MAC address, then you have to go to second method.

1. Go to Start->Settings->Control Panel and double click on Network and Dial-up Connections.

2. Right click on the NIC you want to change the MAC address and click on properties.
3. Under "General" tab, click on the "Configure" button
Click on "Advanced" tab
4. Under "Property section", you should see an item called "Network Address" or "Locally Administered Address", click on it.
5. On the right side, under "Value", type in the New MAC address you want to assign to your NIC. Usually this value is entered without the "-" between the MAC address numbers.
6. Goto command prompt and type in "ipconfig /all" or "net config rdr" to verify the changes. If the changes are not materialized, then use the second method.
7. If successful, reboot your systems.

Method 2:

We can change our MAC Address by editing the registry.

Method 3:

We can change our MAC Address through different Software like SMAC, TMAC etc.

(B) IN LINUX

Spoofing MAC Address

Sending Packets via False MAC Address: Linux

Linux has the ability to "spoof" its own MAC address. I will demonstrate how to "spoof" your MAC with Linux and have that same "spoofed" MAC address occur on each reboot automatically.

All Command in Linux is case sensitive.

Procedure: Set the Parameters and execute: `ifconfig (interface name) hw ether (spoofed MAC address)` From a Linux terminal type `ifconfig` and press the Enter key. The current Ethernet configuration will be displayed, including the MAC address. In this Example: `00:0c:29:4e:1e:cd`



Verify the MAC address against a target by starting a ping command while running ethereal ping 172.16.1.40 From the Ethereal application capture a few packets for verification. Click to highlight an ICMP packet. In this example the results verified the original.

MAC address of 00:0c:29:4e:1e: cd Disable the eth0 NIC typing `eth0 down`. In this Example, the default MAC address was changed by typing: `ifconfig eth) HW ether 11:22:33:44:55:66`



Enable the eth0 NIC by typing `ifconfig eth0 up`. Verify on the Linux machine that the MAC address has changed by typing `ifconfig` and pressing Enter. In this example, the results verify:

1. The new MAC address has been changed to 11:22:33:44:55:66. Repeat the ping process as above to validate the new results across the network. Repeat the Ethereal process as above. In this example, the results:

2. Verify that the new MAC address of 11:22:33:44:55:66 travels across the network.

To automatically have the eth0 NIC run with a "spoofed" MAC address open:

`/etc/sysconfig/networking/devices/ifcfg-eth0`

Edit the `BOOTPROTO= dhcp` line to `BOOTPROTO = none`. Save and close the file to prevent the eth0 NIC from activating on boot. Open the `rc.local` file for editing at: `/etc/rc.d/rc.local`. Add the "spoofed" MAC Address by typing: `ifconfig eth0 HW ether 12:34:56:78:90:10`



If the machine requires a DHCP connections to obtain an IP address:

1. Type the line: `/sbin/dhpcpd eth0`.
2. Save and close the file.
3. Reboot the Linux machine and the new "spoofed " MAC address will be used.

Altering the MAC Address: VMware Workstation

Description: VMware Workstation is perfect for "spoofing" a MAC address as the computer itself is completely virtual. Even though VMware Workstation uses a configuration file to identify which MAC address will be used, this file can be edited to the user's choice.

IV.NEED FOR MAC SPOOFING

1. Protect Personal and Individual Privacy. Some companies track users via their MAC Addresses... In addition, there are more and more Wi-Fi Wireless connections available these days, and Wireless

network security and privacy is all about MAC Addresses...

2. Perform Security Vulnerability Testing, Penetration Testing on MAC Address based Authentication and Authorization Systems, i.e. Wireless Access Points.
3. Build "TRUE" Stand-by (offline) systems with the EXACT same Computer Name, IP, and MAC ADDRESSES as the Primary Systems. If Stand-by systems should be put online, NO arp table refresh is necessary, which eliminates extra downtime.
4. Troubleshoot Network problems. Arp Tables, Routing, Switching.
5. Troubleshoot system problems.
6. Test network management tools.
7. Test incident response procedures on simulated network problems.
8. Test Intrusion Detection Systems (IDS), whether they are Host and Network Based IDS.
9. If for whatever reason you need to keep the same MAC address as your old NIC, but your old NIC failed..
10. Some software can ONLY be installed and run on the systems with pre-defined MAC address in the license file. If you need to install one of this software to another system with a different Network Interface Card (NIC) because your NIC is broken, SMAC will come handy. However, you are responsible to comply with the software vendor's licensing agreement.
11. Some Cable Modem ISP's assign IP addresses base on the PC's MAC addresses. For whatever reason, if you need to swap 2 PC's regularly to connect to the cable modem, it would be a lot easier to change the MAC addresses rather than to change Network Interface Card (NIC).

V.VULNERABILITY

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 they found is secure, s/he may use MAC spoofing to gain access to this network depending on the level of security in use.
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, do 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 re-register 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 WiFi networks, even if they use secure WEP/WPA Encryption

VI.COUNTER MEASURES

1. Our OS is static but it should be dynamic so that it provide a utility that check after few second if any entry found in "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\0001 or 0005" with the name "network address" then the utility should delete it automatically.
2. 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.
3. 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.
4. 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. Higher end AP's support IPSEC.

VII.FUTURE SCOPE

1. Spoofing is possible because the IEEE 802.11 standard does not provide per-frame source authentication, 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. We thus believe this paper will help shed light on how spoof detection can be done and its empirical effectiveness.

2. Our OS is static; in future it might be dynamic which will resolve many "Spoofed based Attack" problems. Such that it might possible that we get the OS which will recheck it's MAC Address after every small interval.

VIII. CONCLUSION

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 with this our MAC can not be spoofed. Presently we are working with the software which will check the registry after every few second if there is any entry with name network address then it will delete it.

IX. GLOSSARY

MAC	Media Access control
NIC	Network Interface Card
ARP	Address Resolution Protocol
LAN	Local Area Network
IP	Internet Protocol
OS	Operating System

REFERENCES

- [1] David C. Plummer, "An Ethernet Address Resolution Protocol", RFC-826, Network Working Group, November 1982.
- [2] Charles 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] MARK D. Spivey, "Practical Hacking techniques and countermeasures",
- [5] SMAC: <http://www.klccconsulting.net/smac>
- [6] Packit: <http://www.snapfiles.com/php/download.php?id=108158&a=7123150&tag=592777&loc=1>
- [7] VMware Workstation: <http://www.vmware.com>
- [8] YANG LIU, KAIKUN DONG, LAN DONG, BIN LI, "Research of the ARP Spoofing Principle and Defensive Algorithm", INTERNATIONAL JOURNAL OF COMMUNICATIONS.
- [9] Min-kyu Choi¹, Roslin John Robles¹, Chang-hwa Hong², Tai-hoon Kim¹, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering, Vol.3, No. 3, July, 2008
- [10] Arbaugh, William A., Shankar, Narendar, and Wan, Y.C. Justin. (2001). your 802.11 wireless networks have no clothes.
- [11] http://en.wikipedia.org/wiki/MAC_spoofing