Volume: 03, Issue: 05, Pages: 1358-1361 (2012)

Counter Measures to Combat Misuses of MAC Address Spoofing Techniques

Alok Pandey
Sr. Systems Manager, Birla Institute of Technology (Mesra), Jaipur Campus, Jaipur, Rajasthan, India
Email: alokpandey1965@yahoo.co.in
Dr. Jatinderkumar R. Saini
Associate Professor & I/C Director, Narmada College of Computer Application, Bharuch, Gujarat, India
Email: saini_expert@yahoo.com

----------ABSTRACT----------

In a computer network several communicating devices are connected to a common shared communication medium. A network interfacing card or a wireless network card is typically used to connect computers on a network. This gives rise to the need of unique identification mechanism to be followed for each of the connected devices. Media Access Control (MAC) addressing is used to properly identify communicating devices. The term MAC spoofing refers to a situation when somebody changes the MAC address of his computer or the network communicating device to impersonate someone else based upon this MAC address identification. Although MAC spoofing may be essential in some situations yet it has become potential threat for the network security as it sets ground for formulating and launching different types of Attacks like ARP Spoofing, DNS Poisoning, Denial of Services, Session Hijacking, Man in the Middle Attack etc. on a network. The purpose of this paper is to spread the awareness about MAC addressing, MAC spoofing techniques normally used, different types of attacks that can be based upon MAC spoofing and some of the counter measures that can be adopted by common network users.

Keywords - **ARP, MAC, MAC Spoofing, NIC**

Paper submitted: December 05, 2011 Date of Acceptance: January 29, 2012

I. INTRODUCTION

When communicating on a network all the devices need to be properly identified for a fruitful and valid communication between the devices. So they need to be identified as sender and receiver and hence the need for source address and destination address came-up. Different companies used different addressing schemes to identify their equipments and devices.

As different technologies developed and several companies started manufacturing the communication devices, a strong need was felt to standardize their identification mechanism and to have a common addressing scheme which could be used to identify these different communication devices their types, manufactures and other related details on the networks. One such mechanism that has now been standardized by IEEE is the Media Access Control Address (MAC) addressing scheme.

A Media Access Control address (MAC address) is a unique identifier assigned to network interfacing devices for communications on the network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer. The MAC addressing scheme acts as a permanent world wide identification mechanism assigned to Network interface card (NIC) & other networking equipment by their Manufacturers. The MAC address is usually burnt in the hardware by the manufacturer of the device. A MAC address usually encodes the manufacturer's registered identification number and is also sometimes referred to as the burned-in address. It is also commonly referred to as Ethernet Hardware Address (EHA) or Hardware Address or Physical Address. A network node may have multiple NICs and hence will have one unique MAC address per NIC.

The hardware address in the case of Ethernet is 48 bits long [1] and is expressed as a combination of 12 hexadecimal digits. The first/leftmost 6 places pertain to the manufacturer and the last/right 6 places pertain to the numbering of device by the manufacturer [1, 4]. As per the IEEE 802 standards the MAC-48 address are normally written as six groups of two hexadecimal digits separated by hyphen (-) or colon (:) in order of transmission example ab-98-76-54-32-10[8]. The other less commonly used convention uses three groups of four hexadecimal digits separated by dots in order of transmission e.g. ab98.7654.3210 [4]. The MAC Addressing scheme of IEEE 802 is based upon the original scheme of XEROX [1] Ethernet Addressing which is a 48 bit addressing mechanism. The total numbers of MAC addresses that can be used are 2^{48} or 281,474,976,710,656. The administration of these addresses can be done either

Volume: 03, Issue: 05, Pages: 1358-1361 (2012)

universally or locally [3]. In a universally administered MAC addressing scheme the addresses are uniquely assigned to the device by the manufacturer of the device and are burned in the hardware itself.

A normal MAC address looks like this: 01:08:5B: AC: DE: F2. It is composed of six octets [3]. The first half (01:08:5B) of each MAC address is known as the Organizationally Unique Identifier (OUI). In other words it represents the manufacturer. The second half (AC: DE: F2) is known as the extension identifier and is unique to each network card / device within the specific OUI. Simply saying the first three octets identify the organization that issued the identifier (OUI). The following three octets are assigned by the organization so that the device is uniquely identified. The locally administered address is assigned to a device by a networks administrator and does not contain OUIs. The second least significant bit of the most significant byte of the address is used to differentiate between universally administered and locally administered address. If the bit is 0 then the address is universally administered whereas if it is 1 then the address is locally administered [3].

II. WORKING OF MAC SPOOFING

As we communicate on computer networks the message is digitized, fragmented and packed into smaller units called packets for transmission on the medium. Once the packets are formed respective headers and trailers are added which may contain the Layer 3 and Layer 2 Addresses of the source and Destination devices.

The process goes through different layers of the TCP / IP model and accordingly different protocols are engaged for communication (typically TCP/IP and ARP). Address Resolution Protocol (ARP) is used to map a Layer 3 IP address to a Layer 2 MAC address [2]. ARP is a protocol that facilitates the network devices to communicate with the TCP/IP protocol. Without ARP, there is no efficient method to build the datagram Layer 2 destination address [2]. When a frame is placed on the network, it must have a destination MAC address [1].

The ARP cache is used to store the MAC-address to IP-address association of the different communicating devices on the network [1]. Every device on the LAN keeps its own ARP cache or small area in RAM that holds ARP results. Without cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and generates additional traffic on the network which might congest the network. Conversely, unlimited hold times could cause errors with devices that leave the network or change the Layer 3 address. Hence there is a need to constantly update the cache which can be done manually or dynamically.

To dynamically discover the MAC address to the destination device, an ARP request is broadcasted on the LAN [2]. The device that contains the destination IP address responds, and the MAC address is recorded in ARP cache. An ARP cache timer removes ARP entries that have not been used for a certain period of time. Depending on the device, times differ. For example, some Windows operating systems store ARP cache entries for 2 minutes. If the entry is used again during that time, the ARP timer for that entry is extended to 10 minutes. A typical user normally dose not interact with ARP on a regular basis.

Unfortunately ARP also acts as a potential security risk due to ARP Spoofing and ARP Poisoning. ARP Poisoning is a technique that is used by an attacker to inject the wrong MAC-address to IP-address association in the ARP cache [5] and diverting the traffic to the MAC Spoofed communicating device. An attacker forges the MAC address of a victim device and frames are now sent to the spoofed destination device rather than genuine receiver [5].

III. MAC SPOOFING TECHNIQUES

Every Ethernet card has a MAC address burned-in at the factory. At times, there is a need to change the MAC address of the communicating device as per the need of the situation. The procedures to change a MAC address are specific to each operating system. The process to change the Mac address for some of the popular Operating Systems will now follow.

3.1 Changing MAC address in Microsoft Windows

Under Windows, the MAC address is stored in a registry key. To change a MAC address, find the key with `regedit` and change it. Windows XP adds an option to change the MAC address on some network cards under the advanced tab in the network adapter's Properties menu. Several software tools like MACSHIFT are freely available which can be used to spoof the MAC address.

3.2 Changing MAC address in FreeBSD

The `ifconfig <interface> link <address>` command can be used to change the MAC address in FreeBSD

3.3 Changing MAC address in Linux

The `ifconfig <interface> hw <class> <address>`, or the GNU MAC command can be used under Linux to change the MAC address of the network device.

3.4 Changing MAC address in Solaris

One can change the MAC address with the `ifconfig <interface> <ether> <address>` command In Solaris.

3.5 Changing MAC Address in Hardware

Some companies like Speed Demon Adapters sell network cards which give you the ability to change the MAC address stored in their EERPROM. This gives the ability

Volume: 03, Issue: 05, Pages: 1358-1361 (2012)

to change the MAC address under any operating system that supports either the PCI bus or PCMCIA.

IV. APPLICATIONS OF MAC SPOOFING

Mac Addresses are permanent addresses and are used for global identification of devices. Surprisingly, it is possible to change the MAC address on most of the hardware. The process of changing the original MAC address of any device to a different one is called as MAC spoofing. MAC spoofing can be helpful in following situations:-

(a) In order to protect the individual's privacy and identification. many companies track users via their MAC addresses. Furthermore, the access to several web based knowledge management sites is also controlled through MAC identifications of the user. In addition, Wireless network security and privacy is primarily based upon MAC Addresses [6]. Hence in order to secure & provide privacy MAC identification plays an important role. Under such conditions in the event of equipment failure it becomes necessary sometimes to spoof your own MAC ID and replace the MAC ID of the newly replaced device with the MAC ID of the original failed device so as to maintain immediate connectivity / functionality of the network.

(b) It is an important action to be performed for Security Vulnerability Testing, Penetration Testing on MAC Address based Authentication and Authorization Systems, especially Wireless Access Points.

(c) In order to have a true Standby offline system with exactly the same Computer Name, IP Address and MAC address as that of the primary system. This standby system could be pressed into service in the event of malfunctioning or failure of the original system for mission critical application and minimize the down time.

(d) The license management in some software is based upon the MAC Address and IP address of the NIC. In the event of failure of the NIC or for any other reason the software may need to be reinstalled on a different system then spoofing your own MAC address may be helpful in restoring the functionality.

(e) When two PCs need to be swapped constantly for whatever genuine reason and access the internet or any network MAC spoofing becomes an imperative solution as many ISPs grant access based upon the MAC address of the equipment.

(f) Troubleshoot various problems related to Systems, Networks & Network Management Tools, ARP Tables, Routing, Routing Table & Switching.

(g) Test the functioning of both Host Based and Network Based Intrusion Detection Systems (IDS).

V. MISUSES OF MAC SPOOFING

This section highlights upon the misuses of MAC Spoofing.

(a) The MAC Address of the access points and other wireless communication devices are spoofed to gain access to the network.

(b) MAC spoofing is used by Attackers in order to bye-pass the MAC Based Filtering in many firewalls and protection devices.

(c) By using a spoofed MAC address the real information of the malicious user may remain undetected and un-logged by various network services like IDS, Firewall, DHCP Server, Wireless Access Points etc.

(d) By using a Spoofed MAC address the actual culprit goes unnoticed whereas someone else who might be a genuine user gets recorded as the culprit.

(e) Using Spoofed MAC address the attacker may gain access to the network, formulate and launch different types of attacks like Man in the Middle, DOS, DDOS, DNS poisoning, ARP poisoning etc.

VI. COUNTER MEASURES TO MAC SPOOFING MISUSES

(a) Generally the MAC Address is retrieved from Operating System whenever it is required as the MAC Address is also stored in Operating System. Hence in order to prevent MAC spoofing the MAC Address must be retrieved directly from NIC instead from the operating system [6].

(b) The MAC Address contained in the arriving ARP packets should not be checked against the MAC Address stored / recorded in the Operating System, rather it should compared with the MAC Address from NIC. If it doesn't match it should delete the entry from OS or from registry.

(c) The MAC addresses can be locked by introducing the router which supports the MAC filtering [7] and IP Reservation. It is possible to reserve a particular IP Address with a particular MAC address using the DHCP for dynamic IP address allocations. Using this only the desired MAC address device gets that particular IP address.

(d) Use of Encryption in the communication between the wireless PC and access point can be effective to prevent MAC spoofing.

(e) Many higher-end Access Points support IPSEC which can also be used to avoid MAC spoofing [6].

(f) Many Operating Systems store MAC addresses statically. The MAC address stored in registry at "HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Class \ {4D36E972-E325-11CE-BFC1- 08002bE10318} \ 0001 or 0005" with the

name "network address" should be checked from time to time. If any entry is found then it should deleted automatically [7].

VII. CONCLUSION

Although MAC spoofing may be essential requirement in many scenarios for uninterrupted network operations and network management yet it cannot be left unplugged so that the antisocial elements exploit this vulnerability and facilitate the initiating of several kinds of attacks like ARP spoofing, Man in the Middle Attack, DNS Poisoning etc. We believe that the counter-measures suggested here are strong enough to be implemented in the real world to combat the threat posed by MAC Spoofing.

REFERENCES

[1] David C. Plummer, "An Ethernet Address Resolution Protocol", *RFC-826*, Network Working Group, November 1982.

[2] Charles Horning, "A Standard for the Transmission of IP Data grams over Ethernet Networks", *Symbolic Cambridge Research Centre*, Network Working Group, April 1984.

[3] T. Pusateri, "IP Multicast over Token-Ring Local Area Networks", *RFC-1469*, Network Working Group, June 1993.

[4] http://en.wikipedia.org/wiki/MAC_spoofing.

[5] Yang Liu, Kaikun Dong, Lan Dong, Bin Li, "Research of the ARP Spoofing Principle and a Defensive Algorithm", *WSEAS Transactions on Communications, 7*(5), May 2008

[6] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", *International Journal of Multimedia and Ubiquitous Engineering, 3*(3), July 2008, 516-520

[7] Arbaugh, William A., Shankar, Narendar, and Wan, Y.C. Justin, "Your 802.11 Wireless Networks have no clothes", 2001

[8] http://www.iana.org/assignments/ethernet-numbers