Intrusion Detection in Wireless Network using BIOS and Motherboard Serial Number

Hiral Vegda
Lecturer, School of Computer Studies
Ahmedabad University,
Ahmedabad, Gujarat,
India

Nimesh Modi, PhD
I/C HOD, Cyber Security Program,
Department of CS,
Hemchandracharya North Gujarat University,
Patan, Gujarat, India

ABSTRACT
The increase in use of wireless network has changed the view of network security. The wireless network is particularly susceptible due to its cooperative algorithms, features of open medium, dynamic changing topology, and lack of centralized monitoring and a clear line of protection. The traditional way of protecting wireless networks with firewalls and encryption software is not enough. The current trend in wireless security shows that new types of attacks are evolving at a fast rate and as many intrusion detection techniques have been developed on fixed wired networks but have been turned to be inapplicable in this new environment so, we need to search for new architecture and mechanisms to protect wireless networks and mobile computing applications. This paper firstly indicates the history of intrusion detection, then the problem in using MAC address as unique identification and then how BIOS, motherboard serial number can be used for intrusion detection.

General Terms
Wireless network security

Keywords
Wireless Network, Intrusion Detection, MAC (Media Access Control) Spoofing, BIOS (Basic Input Output System) Filtering, Motherboard Serial Number.

1. INTRODUCTION
A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations [1].

Wireless networks can be accessed by any computer within range of the network's signal so information transmitted through the network (including encrypted information) may be intercepted by unauthorized users.

Wireless networks should employ a security solution that includes an intrusion detection system (IDS). This paper will describe the need for wireless intrusion detection system and how BIOS serial number will be used to provide security in intrusion detection systems.

Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.

2. Wireless Standards
The wireless standard is commonly represented as 802.11 and is used to setup wireless local area networks (WLANs) in environments such as schools and offices. 802.11 standards have 3 leading protocols (or extensions) as follows [2]:

- 802.11a - It offers higher speed (up to 54-Mbps), more channels and less interference.
- 802.11b - This protocol is also popularly known as "Wi-Fi". This is the standard that was used in most of the Wi-Fi hotspots.
- 802.11g - This is similar to the 802.11b protocol but provides much faster transmission.

3. WIRELESSNETWORK COMPONENTS
A wireless network comprises of the following 3 basic components:

1. Wi-Fi Radio Device: This can be any device that has a wireless card (NIC) built into it such as a laptop, tablet, Wi-Fi enabled PC or a cell phone.

2. Access Point: This is the device which allows Wi-Fi radio devices to connect to the Wireless network using Wi-Fi- standards. The AP then has a wired connection to the Router. However, most modern routers now come with built-in APs to eliminate the need for an extra device.

3. Gateway: Routers are connected to the gateways which then connect the whole Network to the Internet.

4. INTRUSION DETECTION SYSTEM
Intrusion detection systems (IDS) are a weapon in the arsenal of system administrators, network administrators, and security professionals, allowing real- time reporting of suspicious and malicious system and network activity[3]. While they are not perfect and will not show you every possible attack, IDSs can provide much-needed intelligence about what's really going on your hosts and your network. IDS are not stand-alone protection system, but part of an overall protection system that is installed around a system or device [3]. IDS come in a variety of flavors. There are network based (NIDS) and host based (HIDS) intrusion detection systems [4].

4.1 Types of IDS

There are different types of IDS available: IDS that simply monitor and alert and IDS that perform an action or actions in response to a detected threat.

- HIDS

Host Intrusion Detection Systems scans the host systems for activities. Typically, the HIDS scans the operating system log files, or DBMS log files for activity traces. The results of the scan performed by the HIDS are logged into a secure database and compared with the knowledge base to detect any malicious activity.

- NIDS

Network Intrusion Detection System is an IDS responsible for detecting inappropriate, anomalous, or any other kind of data which may be considered unauthorized or inappropriate for a subject network. A NIDS is designed to receive all packets on a particular network segment. Most NIDS are pattern based, which means that they require signatures to alert any intrusion attempt.

- Signature Based

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware.

- Anomaly Based

An anomaly is a deviation or variation from the normal or common order, form or rule. Detecting an anomaly depends on what you are specially trying to detect. A baseline or profile is a fundamental requirement for conducting any anomaly detection. In anomaly detection, a profile is created for each user group on the system automatically or manually. The profiles created are then used as a baseline to define the user activity. If any network activity deviates from this baseline, the activity generates an alarm.

- Passive IDS

A passive IDS is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action.

- Reactive IDS

A reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat. Typically this means blocking any further network traffic from the source IP address or user.

One of the most well-known and widely used intrusion detection systems is the open source, freely available Snort. It is available for a number of platforms and operating systems including both Linux and Windows.

5. PROBLEM IN TAKING MAC ADDRESS AS UNIQUE IDENTIFICATION

Each device you own comes with a unique media access control address (MAC address) that identifies it on a network. Normally, a router allows any device to connect — as long as it knows the appropriate passphrase. With MAC address filtering a router will first compare a device's MAC address against an approved list of MAC addresses and only allow a device onto the Wi-Fi network if its MAC address has been specifically approved. The router probably allows configuring a list of allowed MAC addresses in its web interface, allowing to choose which devices can connect to the network [3].

MAC addresses are easy to get, too. They're sent over the air with each packet going to and from the device, as the MAC address is used to ensure each packet gets to the right device. All an attacker has to do is monitor the Wi-Fi traffic for a second or two, examine a packet to find the MAC address of an allowed device, change their device's MAC address to that allowed MAC address, and connect in that device's place. Picking out the MAC address can be done with an excess of freely available security tools, including Nmap, Tmac etc, or can be done manually also.

6. MAC ADDRESS SPOOFING

On Microsoft Windows systems, the MAC address is stored in a registry key. The location of that key varies from one MS Windows version to the next, but find and edit it [6].

- Change the MAC address on Windows (see Fig.1)

  In Windows Operating System go to control panel, select Network and Internet, select Network Connections, Click on Wi-Fi properties, Click on Configure button, Select Advanced tab, From property select Locally Administered MAC Address, then in Value option write the MAC Address of any device.

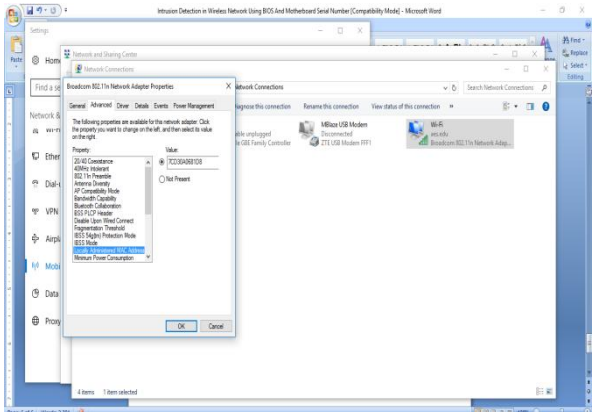

Fig 1: Changing MAC Address on Windows

- Changing MAC Address on Kali Linux Operating System

  Change the MAC address of any device (in wireless network) using the macchanger command on kali linux.

  Example:

  root@kali:# Ifconfig wlan1 down

  root@kali:# Macchanger –r wlan1

  Permanent MAC: 64:66:b3:21:c4:a3(Unknown)

  Current MAC: f8:77:82:29:3d:53(Unknown)

  New MAC: 5c:1d:59:e2:9a:64 (Unknown)

  Explanation:

  -r (random) MAC address will be taken

-m (manual) we have to manually enter the new MAC address

Wlan1 or wlan0 for wireless connection (Wi-Fi) and

Eth0(Ethernet cable) connection

- Change MAC address

  Spoofing a MAC address can be done using Nmap with nothing more than a —spoof-mac command line option for Nmap itself to hide the true source of Nmap probes. If you give it a MAC address argument of "0", it will even generate a random MAC address for you.

- Or, use a GUI Version of software like SMAC, TMAC they provide a one click function to change MAC address on windows machine.

7. USAGEOF BIOS TO GET UNIQUE IDENTIFICATION

As the MAC address is taken as an unique identification of any system, if intruders spoof the MAC address then we are not able to know whether the MAC address has been spoofed by the intruders or not then in that case we have to take other unique identification of system like BIOS and Motherboard serial numbers to identify the unique system.

As already discussed that MAC address can be spoofed, It is not possible to find the unauthorized users (intruders) who are accessing wireless network, So, along with taking MAC address for unique identification of any device like laptop or desktop, take BIOS address for uniquely identification of authorized users. Here in this paper, along with MAC address, take BIOS and Mother board serial number for uniquely identification of a laptop or desktop device. BIOS and motherboard serial number generally can't be changed, it depends on the manufacturer.

Many people want to find out the motherboard manufacturer without having to open the computer. In other cases, such as upgrading the BIOS and seeking drivers for the board, the manufacturer and model of a motherboard must be known.

The motherboard manufacturer can be found through the BIOS serial number. This number is shown onscreen (lower line) during the memory count that is always run when you turn your computer on. If one has never paid any attention, press the Pause key on the keyboard when the memory is being counted and will be able to read the BIOS serial number from the frozen display. The same line contains important information, like the BIOS date.

7.1 Deciphering BIOS Serial Number

The format of BIOS Award's serial number is shown in Fig. 2, where we can see that the first five digits indicate which chipset is used by the motherboard, the next two digits indicating the motherboard's manufacturer and the meaning of remaining digits depends on the motherboard's manufacturer.

Fig. 2: Award Serial Number (BIOS)

Use Command line for getting serial number. Open administrator command prompt in Windows PC. Type in the following command:

wmic bios get serialnumber

8. CODE TO GET BIOS ADDRESS AND MOTHERBOARD SERIAL NUMBER ALONG WITH MAC ADDRESS

To solve this problem, take BIOS serial number and motherboard serial number along with MAC address. Write a program using programming languages like, C, C++ or VB to get the BIOS and Motherboard serial number. Batch file can also be made, which includes the commands for getting BIOS and Motherboard serial number along with MAC address.

Following is the code written using programming language like C to filter the BIOS address:system("getmac"); - This function will give you the MAC address of the system

system("netsh interface ip show address | findstr IP"); - It gives the IP address of the system

system("wmic bios get serialnumber"); - This will give the BIOS serial number

system("wmic csproduct get serialnumber, name"); - It gives the Motherboard serial number and name.

Routers probably allow configuring a list of allowed MAC addresses in its web interface, choosing which devices can connect to our network. So, along with MAC address plan to feed the details of BIOS and Motherboard serial number of each device which are connected to the wireless network to get the unique identification of the system.

There are different open source firmwares(Operating Systems like DD-WRT, OpenWrt) available for routers. Need to install supported Operating System in router.

- For that connect the supported routers (like D-Link, Linksys, TP-Link) in which these open source firmwares can be installed.

- We have to first download the source code of DD-WRT or OpenWrt from the website. Then connect the routers and click on firmware upgrade, there we have to select the file which is downloaded from DD-WRT or OpenWrt websites. So, new firmware will be installed on the router.

- Get the source code of DD-WRT or OpenWrt and edit it to add the BIOS and Motherboard serial number along with MAC address filtering. Once the BIOS and Motherboard serial number is added in the router then we can easily find out the intruders

9. ACKNOWLEDGMENT

We are very much thankful to the IJCA journal for giving us a chance to write paper on our area of interest. We have referred various books and online papers to get the technical knowledge to change the MAC address and how BIOS and motherboard serial number can be used to authenticate the system.

10. REFERENCES

[1] Kirti, "Basic Concepts of Wireless Network", International Journal of Science and Research (IJSR), ISSN 2319-7064.

[2] Available: http://www.webopedia.com/TERM/8/802_11.html

[3] Peng Ning, Sushil Jajodia, xiaoyang Sean Wang. 2001. Abstraction-Based Intrusion Detection In Distributed Environments. ACM Transaction on Information and System Security, Vol. 4, No. 4.

[4] Fadia Ankit, Ebook on Network Security, 2006

[5] Shrikanth Ramesh. 2014. How to Hack Hacking Secretes Exposed. http://howtohack.gohacking.com

[6] Sungmo Jung, Jong Kim, Seoskoo Kim, "A Study on MAC Address Spoofing Attack Detection Structure in Wireless Sensor Network Environment", http://link.springer.com/chapter/10.1007%2F978-3-642-23312-8_4

[7] Hatkar Archana A, Varade Gauri A, Hatkar Arvind P. 2012. Media Access Control Spoofing Techniques and its Counter Measures. International Journal of Scientific & Engineering Research, Volume 2, Issue 6, ISSN 2229-5518.

[8] Pandit Amita, Gond Sunita. 2013. Analysis for Improving Intrusion Detection System in Wireless Network. International Journal of Advanced Research in Computer Science and Software Engineering.http:// www.ijarcsse.com

[9] Takahashi Daishuke, Xiao Yang, Zhang Yan, Chatzimisios Periklis, Chen Hsiao-Hwa. 2010. "IEEE 802.11 User Fingerprinting and its applications for Intrusion Detection", Computers and Mathematicswith Applications.http://www.sciencedirect.com/science/article/pii/S0898122110000131