Building Simple Protection for Wireless-Fidelity Network

Manar Y. Ahmed
Prof. Assist
Dept. of Computer Sciences

Mohammed Zaki Hasan
Lecture Assist
Dept. of Software Engineering

College of Computers sciences & Mathematics

University of Mosul

Abstract

This paper describes some of the attacker utilize to disrupt wireless networks through MAC address, and then perform the simple protection through Traffic Protocol Authentication Module (TPAM). This module perform Challenge-Respond based on the hash part of MAC by using the hashing operation, this challenge will occur between the administrator, and the group of the customers through wireless network, and then generate and captured MAC address for all computers connect to wireless network detection unspecified MAC address, filtering it from the MAC address spooling according to protocol programmed by Visual Java#.Net. At the first stage the generation of MAC addresses must capture by many wireless networks tools such as AirJack, FakeAp and Wellenreiter, through analysis the traces. Then the programmer identifies the techniques which can be employed the used the capability to detect the anomaly MAC address, which also the user must alert the administrator of the wireless networks, or alert the others his/her friends in same workgroup. Wireless access points have large scale of the security problems, one of them are the suffering the unauthorized access and use. So the administrator or the wireless network should deal with his/her others groups to the specified generation of MAC address, and then registered the newest of the overall MAC address of the wireless network.

الملخص

يضيف هذا البحث بعض الهجمات المستخدمة لتعطيل الشبكة اللاسلكية من خلال عنوان سيطرة الوصول للوسط (media access control) ومن ثم إيجاد وسيلة تقنية حماية مبسطة من خلال نموذج بروتوكولي التحقيق (Mac) هذا النموذج يحقق (الاستجابة والتحدي) (chanllege reply) بالاعتماد على جزء الدالة الهاشية من Mac هذا التفاعل سوف يحدث بين مدير أدارة الشبكة ومجموعة من العملاء والزبائن خلال شبكة لاسلكية ، بالحصول على جميع عناوين سيطرة الوصول للوسط (Mac addresses) لجميع الحاسبات المرتبطة بالشبكة اللاسلكية وتحديد العنوان المشكوك فيه ، وترسيخه من بقية العناوين من خلال بروتوكول معين ثم برمجته باستخدام visual java.net تم الحصول على عناوين سيطرة الوصول للوسط من خلال استخدام أدوات الشبكة اللاسلكية مثل FAKEAP,AIRJACKو.... ، من خلال تحليل المسارات . بعد ذلك يحدد المبرمج التقنية التي يمكن أن يستخدمها لكشف عنوان Mac المشكوك فيه ويجب على المستخدم تنبيه مدير الشبكة أو زملائه ضمن نفس المجموعة . نقاط الوصول للشبكة اللاسلكية تملك مدى واسع من مشاكل الأمنية من ضمنها هي معاناة الاستخدام والوصول الغير المخول للشبكة . لذلك على مدير الشبكة إن يتعامل مع مجموعته مع توليد محدد من عناوين الوصول ، وتسجيل عنوان الوصول الجديد للشبكة .

1. Introduction

1.1. Media Access Control address (MAC):-

Each computer attached to an Ethernet is assigned a unique 48-bit (6 bytes) integer. Every company is responsible for ensuring that every manufactured unit gets a unique address within its assigned range of addresses. Thus, no two cards will purposely have the same address [4]. The construction of the MAC address consists from

- The first 3-bytes from the left of address are used to identify the manufacturer of the Network Interface Card (NIC).
- The last 3-bytes of address are the unique serial number. The table below shown the NIC serial numbers for some companies, which almost today used the Electrically Erasable Programmable Read Only Memory (EEPROM), to the store the information into it.

Manufacturer	Model	EEPROM	Mac Address	Data
National Semiconductor	NSC	93LC06	08:00:17:03:c0:e5	0800 0317 e5c0 0000 0500 010d 010a 5757 4242 0000 0000 0000 0000 0000 0020 0020
Ansel Communication	N200 Plus 3	93C46	00:40:90:80:07:7e	4000 8090 7e07 ffff ffff ffff ffff 5757 4242 ffff ffff ffff ffff ffff 0100 ff20

Table 1: NIC serial numbers for some companies

There are many different manufacturers of the Ethernet Controllers. All most used a National Semiconductor DP83905-EB AT/LANTIC, which interfaces to an ISA bus [3]. Other devices include Realtek RTL8129 and RTL8029 fast Ethernet Controller, designed for interface to a PCI bus, the standard Microsystems LAN9000-family and the UMC UM9003[4].

The EEPROM is programmed during card manufacture and placed onto the board. In some cases, the serial EEPROM is programmed directly from the Ethernet controller, so that the MAC address and other configuration information can be entered via personal computer (PC) software.

For this ability of the changing or erased and the written up without error, the attacker can have a best chance to attack the wireless network, and may make access denial of services for the subscriber. There are different software available for the changing the Media Access Control, addition to the system software such as the operation system (i.e. windows edition) give the ability to erase the original value of the MAC address through setting a new configuration to the MAC address. Another way can change their MAC with "ifconfig" tool or with short C program calling function to alter the value of Media Access Control. Nearly all 802.11 cards in use permit their MAC to be altered, often support and derivers from the manufacturer [4].

1.2. Managing the database of MAC addresses:-

It is simply to build the database for Media Access Control; the entries of the database will change daily, because the unknown of the subscriber in the wireless network. For advance building the database more others things required such as the temporary network access by visitors, vendors, or contractors requires changes to the database to grant access, and perform the changing to remove the access to wireless network, and others things. To enter the information into the database the administrator need some basic information from the user to register the connection, and others information, such as the data field that contain challenge-respond hashing values between the Administrator and his/her subscribers.

There are many benefits of the creation database of Media Access Control:-

- It helps the Administrator to understand the follow steps for the attacker which sends data from an arbitrary source address and not except to see a response to their actual source IP address.
- It permits the Administrator to use the basic form of access control on wireless network, to configure access points or

neighboring routers to permit only registered MAC to communicate on the network.

- It is useful to detecting the normal matching user authentication credentials to the source MAC address of a client. Also it can detect the anomalous MAC address.

1.3. Detecting Anomalous Media Access Control:-

A hardware manufacturer wishing to produce network cards needs to obtain a three-byte organizationally unique identifier from the Institute of Electrical & Electronics Engineers (IEEE) to be used as a prefix for MAC address of their products [3]. So according to Wellenreiter technique, it can permit the subscriber to register as first time access to wireless network with MAC generates as 4 random values between the prefix "0x00" and postfix "0xFF". Both the prefix and postfix values consider as key generation between the administrator and their subscribers, to acceptance the connection, before the unauthenticated and unassociated. At this moment the administrator begin to check out the database for MAC address through the command network tool such as "ifconfig". Then the associate with target access point from the access point. From these information, it can the administrator detect the anomalous MAC based on their both prefix and postfix information. But another problem found that if the thief known the dealing generating key between the administrator and his/her subscribers, then it important to add new additional features to increasing the level security at the normally situation. This adding operation consists from sub operations, hashing the part that surrounded between the both prefix and postfix, i.e. the remaining 4 random values, and challenge-response the request of the administrator, that will describes in paragraphs below.

2. Wireless Networks

2.1. The structure of wireless-Fidelity (Wi-Fi):-

A wireless-Fidelity (Wi-Fi) network will gives nearby computer enthusiasts an opportunity to break into the attacked wired network. The most critical security

vulnerability damaging Wi-Fi was published in 2001[7]. The attacker has improved, refine and combine in software tools that automate portions of the attacks. So the poorly secured Wi-Fi networks can be utilized to attack networks and corporations from the inside, instead of attempting to do it externally from the internet. Attacks exploiting link-layer protocol vulnerabilities require a different set of intrusion detection mechanism. Most link-layer attacks in WLANs are denial of service, attacks and work by spoofing either access points (APs) or wireless stations. Spoofing is possible because the IEEE 802.11 standard does not provide per-frame source authentication, but can be effectively prevented if a proper authentication is added into the standard [4]. Even if provided in the (i.e. the authentication without perfect technical) next-generation of WLANs equipments, it cannot protect the large installed base of legacy WLAN devices from the different attacks [7].

One attack techniques can take this form of attacking through the targeting MAC address spooling, where the MAC address used as singularly unique at the layer two. MAC addresses are globally unique for all LAN-based devices in use today. It may not good idea in many cases to use the MAC address as an authentication, because the attacker targeting wireless LANs utilize the ability to change their MAC address to circumvent [5].

The 802.11 standard define two different operator modes in the wireless network: the Station (STA) and Access Point (AP). A wireless network, or Basic Service Set (BSS) as it is referred to in the standard, may be created in two configurations: the Independent Basic Service Set (IBSS) and the Extended Service Set (ESS). An IBSS, or Ad-Hoc network, is created by any number of stations without requiring any Access Points. for this paper, the choosing of the infrastructures mode it better than the Ad-hoc mode. Because of the infrastructure mode, each client sends all of its communication onto the central station, or Access Point (AP). The AP acts as Ethernet Bridge and forwards the communication into the appropriate network, either the wired network, or the

wireless network. As shown in the figure1. Prior to communication data, wireless clients and APs must establish a relationship, or an association between the clients and the APs. The association process is two steps involving three states [2, 8]:-

- Unauthenticated and Unassociated.
- Authenticated and Unassociated
- Authenticated and Associated

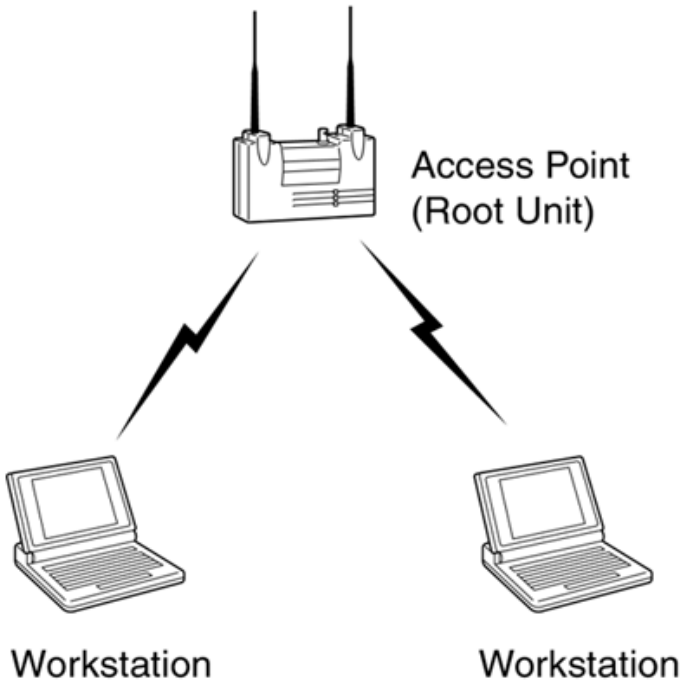

Figure 1: example of infrastructure network

2.2 Finding & opening both access point & system connection :-

One way to find the wireless client and associating with an access point is, all access point transmit a beacon management frame at fixed interval. To associate with access point and join a Base Station Service (BBS), client listens for beacon messages to identify the access point within range. The client then selects the Base Station Service (BBS) to join in a vendor independent manner [6].

Open system authentication is the default authentication protocols for 802.11. This additional protocol based to shared key and then using the standard the challenge and respond for MAC along the connection to open system, a client is authenticated if it simply responds with secret key based to the complexity degree of static mathematical function [1]. The Administrator sends an authentication request, through the beacon of the access point for all the subscribers on the wireless network to indication the MAC. But this request based on the function challenge which deals between the Administrator and his/her subscribers, the responder responds by send the answer of this challenge. Sometime this system named as a one-time password that is changes every time it used, or the accessing to wireless network instead of assigning a static phrase to a user, the system assigns the a static mathematical function. So in order to open the connection safely between the administrators and their groups, first arrogations the same prefix and postfix of MAC as the secret key, and then the system provides an argument to function, and then the subscribe computes the function value and returns it, i.e. the MAC address with new hashing value. The proof of function will be on one-sided, for example, with this function f(x) =x+1, the system prompts with a value for x, and the subscribers computes the value of x+1, this kinds of mathematical functions used for authentication techniques are response quickly and easily, from subscribe. [6]

So the administrator demands certain identification of the user. This identification describes as id and password, which it is the hash value of MAC address. An interruption of the connection immediately occurs once when the administrator recognizes the attacks from in or outside network. Both figures below showed the infrastructure network topology, and the structure of the challenge system between the server and its client. The challenge begins with a beacon to registers the all subscribers in range of wireless network, then the administrator starting with challenge system to authentication the access of user,

and opening connection, or otherness, disconnect the connection after detect any intrusions.

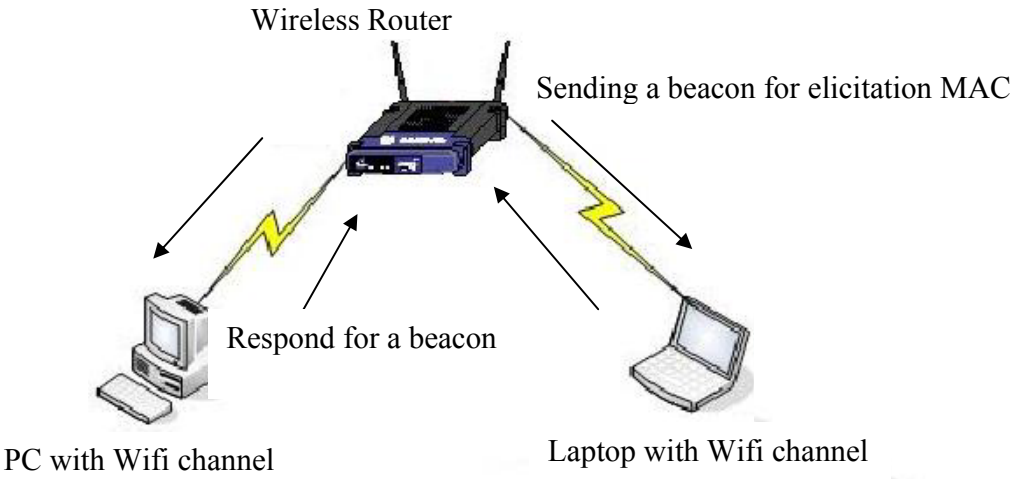

Figure 2: infrastructure network

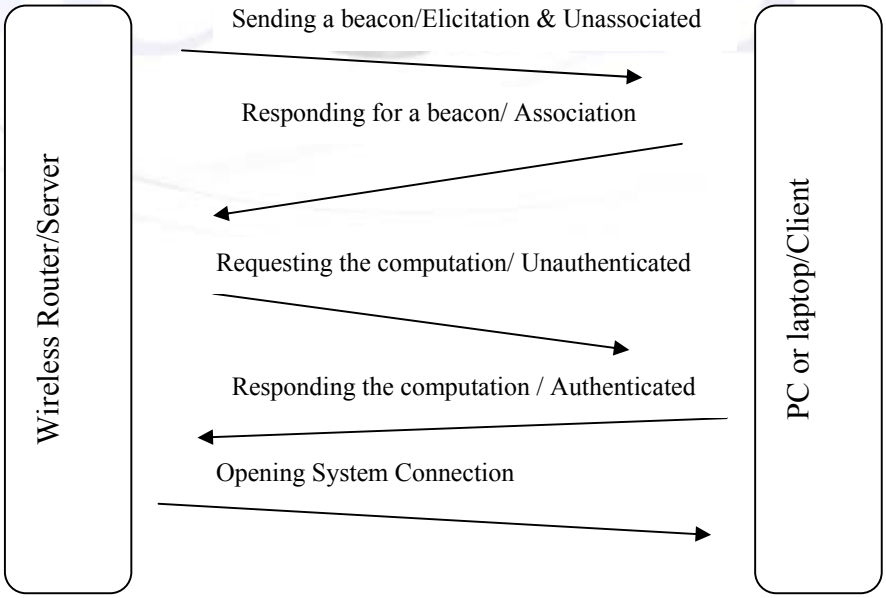

Figure 3: Traffic Protocol Authentication Module

3. The Integrated Development Environment (IDE) of the Challenge System:-

Traffic Protocol Authentication Module (TPAM) programmed by Visual Java#.Net. At the first stage the generation of MAC addresses must capture. Then the programmer identifies the techniques which can be employed the used the capability to detect the anomaly MAC address, which also the user must alert the administrator of the wireless networks, or alert the others his/her friends in same workgroup, as shown figure 4 below.

The challenge system that performs consists from simple computation of hash function that agrees both the administrator and user about the hash function and its parameters as key to authentication and opening the connection channel for subscribe. Any disclosure of the hash function key, the administrator has permission to disconnect the connection filtering the anomaly MAC address. Then reply the beacon signal with newest hash function key.

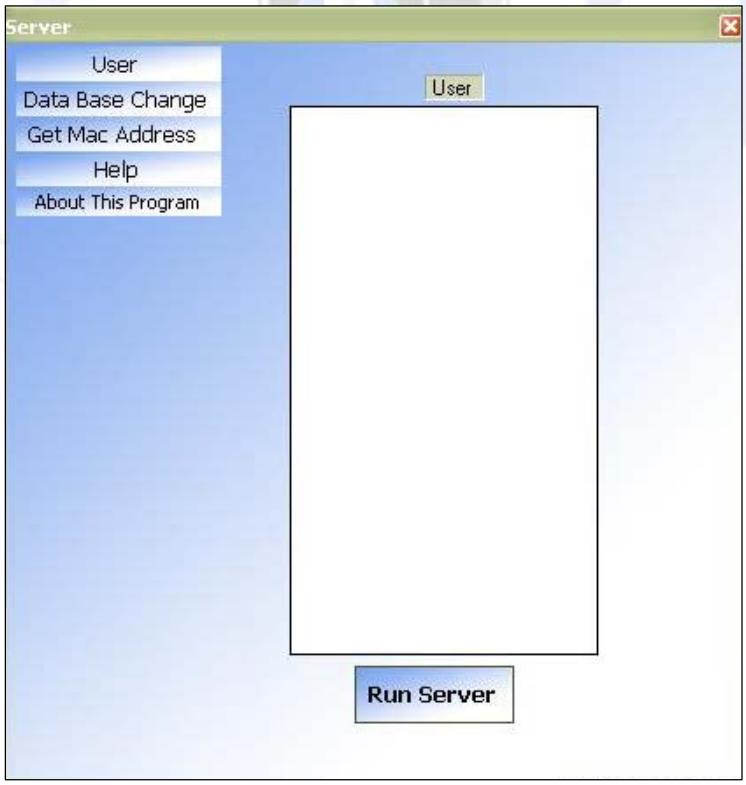

Figure 4: The IDE of the Traffic Protocol Authentication Module (TPAM)

4. Conclusion:-

The combination between the generation and the challenge response, it supporting wireless network to increasing the level security mechanism at normal situation, but may be either be weakness in cases, from the series of attacks can disclosure the function key generation, or others cease more difficult to user to respond to the request in order to establish the connection. This come from the using more complexity degree of the hash function. So the deal must occur between the administrator and their groups about, and the administrator has a high privilege to disconnect and locking the MAC.

5. References:-

1. Charles P. Pfleeger, "Security in Computing ", the University of Tennessee, Prentice-Hall, Inc. 1989.
2. Dino A. Dai Zori, Shane A. Macaulayddz@theta44.org, ktwo@ktwo.ca , March 18,2005.
3. Fanglu Guo & Tzi-cker Chiueh, "Sequence Number-Based MAC Address Spoof Detection", computer science department, stony brook university, NY 11794, the website http://fanglu,chiueh@cs.sunysb.edu.
4. Interworking with TCP/IP, Vol. 1, Douglas Comer, pg. 25, ISBN 0-13-468505-9.
5. Joshua Wright, GCIH, CCNA, "Detecting Wireless LAN MAC address spoofing", Joshua.Wright@jwu.edu, the website http://home.jwu.edu/jwright, 1/21/2003.
6. T.Rikure, A.Jurenoks, "WIRELESS NETWORK TECHNOLOGIES IN TRANSPORT AREA: SECURITY AND E-LEARNING APPLICATIONS", Wireless technologies, security, wireless enabled teaching, application, IEEE 802.11b specification, LAN, 2004
7. The Nowires Research Group, the website http://www.nowires.org.
8. William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes",Department of Computer Sciences, University of Maryland , College Park, Maryland 20742, March 30, 2001.