Wireless network security

November 28

2012

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks.The first line of defense for your Wi-Fi network is encryption, which encodes the data transmitted between your PC and your wireless router.

BY Electrical engineer :

Mariwan Omar Saleh

This Project is submitted for getting adviser degree in electrical engineering.

WIRELESS SECURITY

ABSTRACT - Secured wireless computer networks are more important because signals are available through air and it's easier to attacks from passive eavesdropping and active interfering. Now it was suffered from more problems, one from these problems is attach from the users and hackers. Therefore, wireless computer networks security is very important to solve or decrease this attach, a lot of researches were worked improved wireless security in this field but in different ways and different methods.

This project had been represented how to prevent hackers' accessing to the server, by using encryption to media access control "MAC address" from the two ends (server and user), using RSA public-key cryptosystem..

***Keywords*:-** Wireless Security, MAC Address , RSA Public-Key Cryptosystem..

1. INTRODUCTION

Data signals are transmitted from one device to another using one or more types of transmission media, including twisted-pair cable, coaxial cable andfibre -optic cable. A message to be transmitted is the basic unit of network communications. A message may consist of one or more cells, frames or packets which are the elemental units for network communications. Networking technology includes everything from local area networks (LANs) in a limited geographic area such as a single building, department or campus to wide area networks (WANs) over large geographical areas that may comprise a country, a continent or even the whole world.

According to Sumathy and Kumar, Active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data.

External attacks are typically active attacks that are targeted to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls and encryption techniques.

2. WIRELESS NETWORKING

The wide wireless networking is the various types of 2.4 GHz WiFi devices, is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations .

There are two ways to verify wireless networking through IP address (Internet Protocol) or MAC address.

3. MAC ADDRESS

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following formats . MM:MM:MM:SS:SS:SS MMMM-MMSS-SSSS

The first half (24 BITS) of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half (24 MORE BITS) of a MAC address represents the serial number assigned to the adapter by the manufacturer.

Recall that TCP/IP (Transmission Control Protocol/Internet Protocol) and other mainstream networking architectures generally adopt the OSI model (Open Systems Interconnection). In this model, network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in the OSI model). They allow computers to uniquely identify themselves on a network at this relatively low level as shown in Fig. (1).

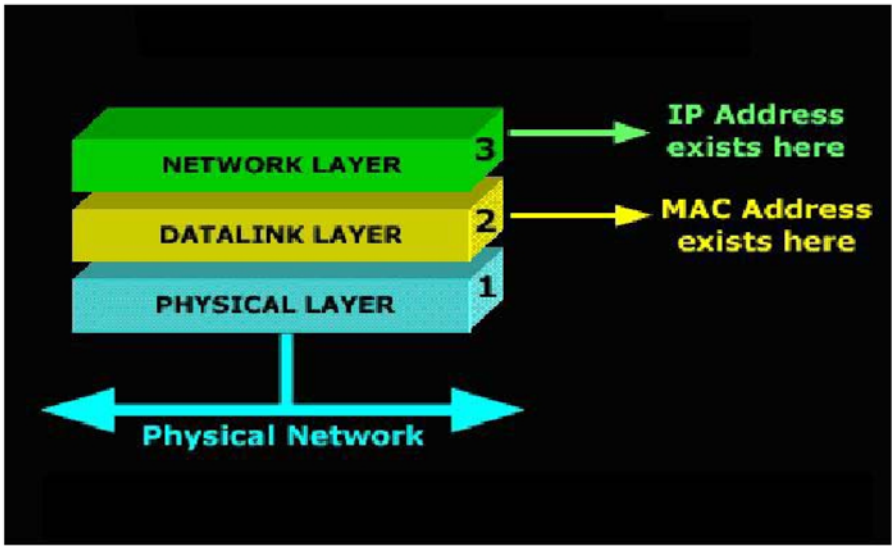

Fig. (1): First Three OSI Layers

4. WIRELESS SECURITY

There are many ways to protect the user or computers from hackers, like user name, password … etc, in this work are taken some options can hackers or hacker's program that enter to the network, this option is MAC address.

The operation of connection between the server like "Mikrotik server" (that's wide used in our country) and user by IP address as shown in figure (2), this connection happen when the user send message to access point and through access point to the server, server are register the new user by (user name and password), after this operation the connection are continue, and many packets of data are translated between server and user, one of properties of Mikrotik server, is the server deals with MAC address of user not with IP address after connection because the MAC address are represent the physical address, when the user are stooped or separate from the server in few minutes, the hacker is connect with the server by taken the user's MAC address (through some of program).

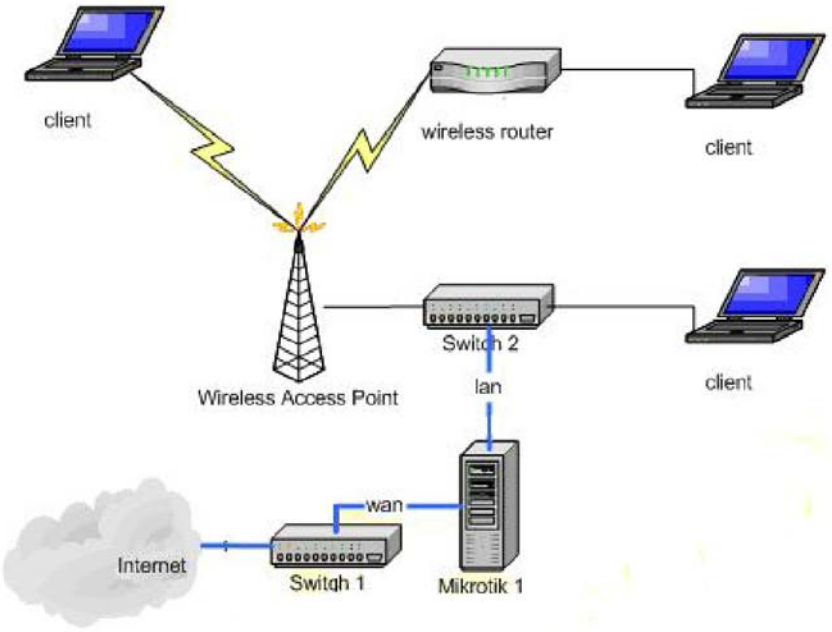

Fig. (2): Basic network topologies

5. PROPOSED SYSTEM

5.1. STEPS OF SECURED SYSTEM

The steps of proposal system for wireless networking by the RSA public-key cryptosystem are:-

1- Register user's MAC address in Mikrotik server.
2- Encryptions MAC address.
3- Send crypto MAC address through access point.
4- Receive Crypto Mac address from server.
5- Decryption MAC address in user's computer.
6- Encryptions MAC address.
7- Send crypto MAC address through access point.
8- Receive Crypto Mac address from user.
9- Decryption MAC address in Mikrotik server.

Figure (3) shows the flowchart of the steps of secured system.

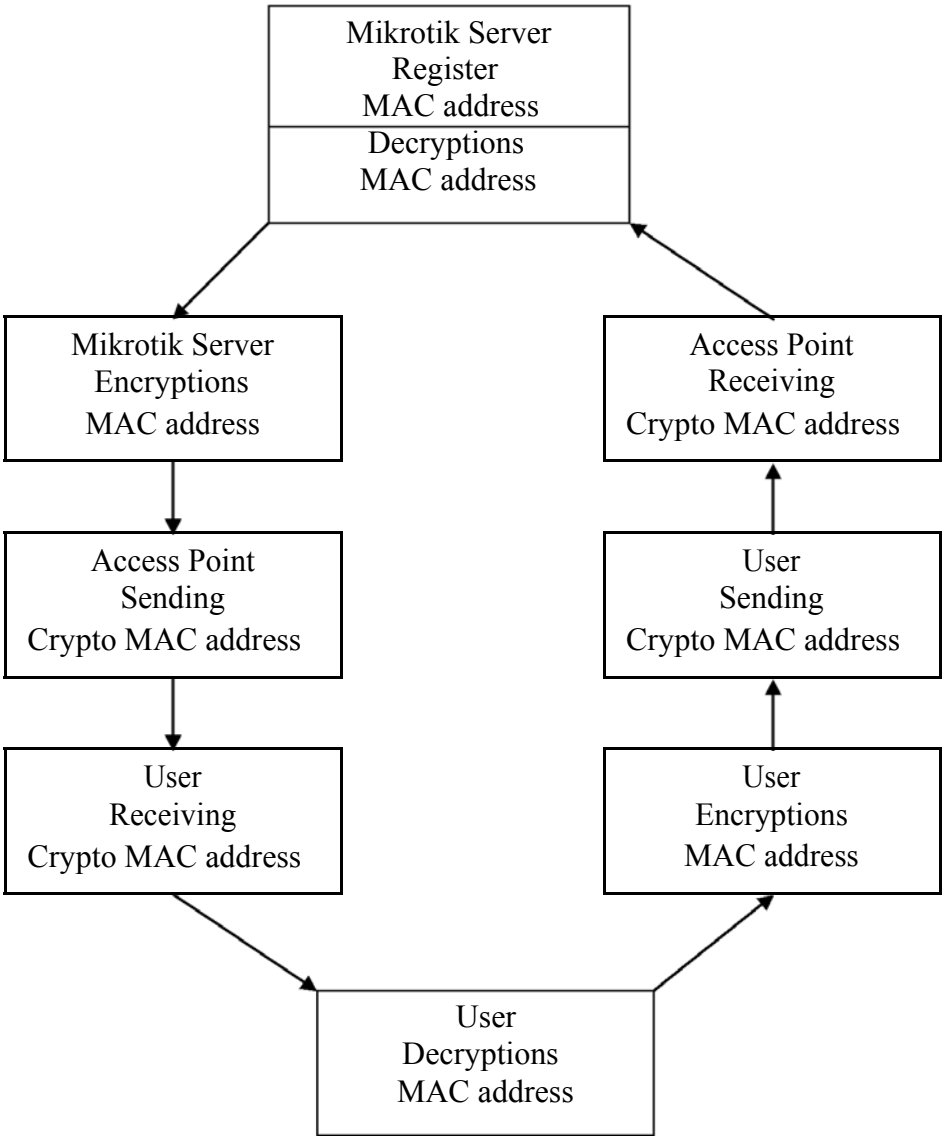

Fig. (3): Flowchart of proposal system

5.2. STEPS OF RSA PUBLIC KEY CRYPTOSYSTEM

The steps of RSA public key cryptosystem are:

1- Generate two keys (public key (e, n) and secret key (d, n)).

a- each reserve generate three numbers:

p , q (large primary numbers) and lets 3, 17 respectively and e

(large number), lets 5.

b- Then calculate public key (e, n):

n = p *q = 51, the public key (5, 51)

c- Then calculate secret key (d, n):

$d = e^{-1} \bmod \Phi(n)$

Where $\Phi(n) = (p-1)(q-1)$, $\Phi(n) = 32$

$d = \frac{GCD(\Phi(n)) \cdot \Phi(n) + 1}{e}$, where GCD (2, 16) = 2 (Greatest Common Divisor)

d = 13, the secret key (13,51).

2- Encryption MAC address, the proposal MAC address are :

11-22-33-AA-BB-FF

In this work are the numbers from (0 to 9) and the characters (A to F) are (10 to 15), each of MAC address are encryption as (m1, m2, …, m12) to (c1, c2, …, c12) by:

$C_1 = M_1^{\,d} \pmod n$, $C_1 = 1^{13} \pmod{51} = 01.$

C_3 & $C_4 = 2^{13} \pmod{51} = 32.$

$C_5C_6 = 3^{13} \pmod{51} = 12.$

C_7 & $C_8 = 10^{13} \pmod{51} = 28.$

C_9 & $C_{10} = 11^{13} \pmod{51} = 41.$

C_{11} & $C_{12} = 15^{13} \pmod{51} = 36.$

Now have encryption MAC address is represented by:

0101-3232-1212-2828-4141-3636

3- Decryption MAC address, after encryption MAC address the user are received it and decrypt MAC address by using:

$M_1 = C_1^{\,e} \pmod n$, $M_1 = 1^5 \pmod{51} = 01.$

C_3 & $C_4 = 32^5 \pmod{51} = 02.$

$C_5C_6 = 12^5 \pmod{51} = 03.$

C_7 & $C_8 = 28^5 \pmod{51} = 10.$

$$C_9 \ \& \ C_{10} = 41^5 \ (\text{mod}51) = 11.$$

$$C_{11} \ \& \ C_{12} = 36^5 \ (\text{mod}51) = 15.$$

Now get original MAC address (11-22-33-AA-BB-FF), figure (4) illustrated Steps of RSA public key cryptosystem.

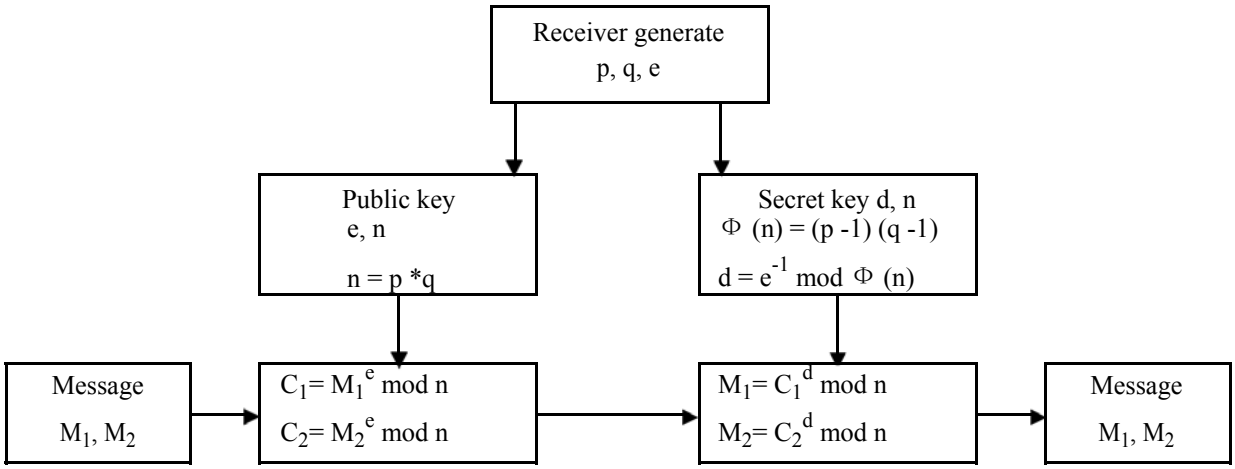

Fig (4): Steps of RSA public key cryptosystem.

6. There are two primary security issues:

* Access - making sure that only authorized people can use the wireless network. Without proper access control anyone in the vicinity of the building can use the wireless network, and thus get access to net. WEP) and Wi-Fi Protected Access (WPA). WEP is one of the least secure forms of security. A network that is secured with WEP has been cracked in 3 minutes by the FBI.WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length

* Privacy - making sure that no one can watch your communications. Without this, anyone any the vicinity of the building can watch everything you do on a wireless network. This will let them steal your passwords and look at everything you are doing.

6.1 WPA and WEP

WPA and WEP are technologies that "encrypt" the traffic on your network. That is, they scramble it so that an attacker can't make any sense of it. To unscramble it at the other end, all systems using it must know a "key" or password.

Note that WPA is now in a second generation, referred to as WPA2. Unless otherwise specified, this document uses "WPA" to refer to both.

WPA and WEP provide both access control and privacy. Privacy comes from the encryption. Access control comes from the fact that someone must know the password to use your network.

For this reason, for small networks, using WPA is enough to meet the requirements of the Wireless policy. However you will still want to make sure that any services that use a password or other private information use SSL or some other type of end to end encryption.

WEP is significantly less secure than WPA, but can be used until your equipment can be upgraded to support WPA. While WEP is widely regarded as insecure, it is still a lot better than nothing.

WPA has two modes, personal and enterprise. For small installations you'll want to use personal mode. It just requires a password. Enterprise mode is for larger installations, that have a Radius server that will support WPA.

The primary problem with WPA in personal mode is that it has a single password, which you must tell to all users. That becomes impractical for larger installations.

WPA in enterprise mode requires each user to login with their own username and password. That simplifies management in large installations, because you don't have to distribute a common password to all your users. However it is a bit more complex to implement:

WEP

WEP stands for Wired Equivalent Privacy, a standard for WiFi wireless network security. A WEP key is a security code used on some Wi-Fi networks. WEP keys allow a group of devices on a local network (such as a home network) to exchange encoded messages with each other while hiding the contents of the messages from easy viewing by outsiders.

WEP key is a sequence of hexadecimal digits. These digits include the numbers 0-9 and the letters A-F. Some examples of WEP keys are:

* 1A648C9FE2

* 99D767BAC38EA23B0C0176D15

WPA

The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11istandard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP), was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP

WPA2

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark. Wi-Fi devices certified since 2006 support both the WPA and WPA2 security protocols. WPA2 may not work with some older network cards

7. The recommendations below summarize the steps you should take to improve the security of your home wireless network.

7.1Change Default Administrator Passwords (and Usernames)

At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.

7.2 Change the Default SSID

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." True, knowing the SSID does not by itself allow your neighbors to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network.

7.3 Turn on (Compatible) WPA / WEP Encryption

All Wi-Fi equipment supports some form of *encryption*. Encryption technology scrambles messages sentover wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings.

7.4 Enable MAC Address Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the *physical address* or *MAC address*. Access points and routers keep track of the MAC addresses of all devices that connect to them. Many such products offer the owner an option to key in the MAC addresses of their home equipment, that restricts the network to only allow connections from those devices. Do this, but also know that the feature is not so powerful as it may seem. Hackers and their software programs can fake MAC addresses.

7.5 Disable SSID Broadcast

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. In the home, this roaming feature is unnecessary, and it increases the likelihood someone will try to log in to your home network. Fortunately, most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator.

7.6 Do Not Auto-Connect to Open Wi-Fi Networks

Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbor's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user). This setting should not be enabled except in temporary situations.

7.7 Assign Static IP Addresses to Devices

Most home networkers gravitate toward using *dynamic IP addresses*. DHCP technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range instead, then configure each connected device to match. Use a *private IP address range* (like 10.0.0.x) to prevent computers from being directly reached from the Internet.

7.8 Enable Firewalls On Each Computer and the Router

Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider installing and running *personal firewall software* on each computer connected to the router.

7.9 Position the Router or Access Point Safely

Wi-Fi signals normally reach to the exterior of a home. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighboring homes and into streets, for example. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize leakage.

7.10 Turn Off the Network During Extended Periods of Non-Use

The ultimate in wireless security measures, shutting down your network will most certainly prevent outside hackers from breaking in! While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods offline. Computer disk drives have been known to suffer from power cycle wear-and-tear, but this is a secondary concern for broadband modems and routers.

8. CONCLUSIONS

From the dealing with wireless technology, and knowing how hackers are attempt to access to this connection (server) especially what was presented by this proposal system, it can be concluded that:

1- The system is providing one of complex way that prevents the hackers to attack wireless connection.

2- Proposal system is used RSA public key cryptosystem that very difficult when use large primary numbers to make it very complex to solve from hackers.

3- Proposal system give to server more reliability and capability to the users, for using wireless service without any disconnection from the hackers.

4- Many researches development wireless networks in different ways and different methods.

9. REFERENCES

1. B. Pioper, “Internetworking Technology Overview”, June 1999.
2. S. Sumathy and B. Kumar “Secure Key Exchange and Encryption Mechanism for Group Communication Wireless AD Hoc Networks” March 2010
3. http://en.wikipedia.org/wiki/Wireless.
4. http://www.firewall.cx/index.php .
5. http://www.dmasoftlab.com/cont/radman.
6. http://wiki.mikrotik.com/wiki/Initial_MAC_Winbox_Connection .