Security threats to wireless networks and modern methods of information security

Dr.Yasser Elmalik Ahmed Seleman

KINGDOM OF SAUDI ARABIA, MINISTRY OF EDUCATION, BISHA UNIVERSITY

PhD *in Computer Science, Omdurman Islamic University*
M.sc *in Information Technology, Newcastle (USA).*
M.sc *in Information Technology, the National Ribat University*
Email*: Dr.yaserking@hotmail.com*

***Abstract*—** Network is a technology used to connect computers and devices together. They allow people the ability to move easily and stay in touch while roaming the Internet in the coverage area. This increases efficiency by allowing data entry and access to the site. Comparing wireless networks wired networks in terms of cost, we find that wired networks are more expensive due to the cost of the network connections of electricity and running and add computers and change their positions to suit the network supply.

As a result, the use of widespread wireless networks. But there are security gaps in these networks may cause problems for users Security holes intended problem or weakness in the wireless network system may make it easier for hackers to penetrate and steal sensitive data and causing material losses to individuals and companies.

Knowing security holes and contributes significantly to the wireless network is immune from attempts to infiltrate and penetration design

Keywords—**Protocol*:*** Language is between computers connected via the network, in order to exchange information. If we define the language of the Protocol technology, we say that a formal description of the bodies messages and rules that must be followed on two computers to exchange those messages.

I. INTRODUCTION

Wireless networks are a type of computer networks, and is working on the data and information transfer (send - reception) without wires (wirelessly), through electromagnetic waves carry this information.

Important wireless network to protect intruders from access to user information, most people have more than one computer and laptop at home and even phones and key servers and Xbox, and other devices that they use to store their information and their files and family photos and passwords, vulnerable to theft and access to information secret task such as banking bank statements and e-mails. of the most important things that contributed to the technical stability has become and therefore reliable in production in various business environments, especially with the ease of use and price of access points (Access Point) as well as to support wireless networks in portable devices processors and breadth of the spread of this technology, where there is almost devoid home or facility of WLAN access points.

As far as deployment of this technology as far as increase the importance of care by applying security measures to protect wireless networks, and the neglect of this aspect of user data and regulations relating to the wireless network at great risk from hackers and intruders to within it may displays.

The use of wireless networks is increasing dramatically due to the offered integration with modern electronics that are produced in all areas of our daily lives.

The importance of the different networks and their uses:

The networks that have been established precisely one of the most orderly and administrative components that depend on it most of the work because of their key role in the organization of the administrative process in the economic entity of different types, or at home, where networks provide a lot of important solutions, including:

1. Facilitate the exchange of documents and files process.

2. Several common printing methods provide.

3. Provide wireless network to access the Internet through mobile devices.

4-users' computers provide access management and determine their powers.

5-possibility of providing management of web content available at the users control and allow the blocking of sites.

6-connect servers to provide various data and deal with administrative programs that need communication between users.

7-The ability to make a local mail server to send and receive e-mail between the local network users.

8-provide a more flexible and safer operations for data backup mechanisms.

9-saving store shared information and access to centers in multiple ways.

10-saving mechanisms to link the branches over the Internet and the work of the so-called VPN - Virtual Private Network.

Clarify the types of protocols used and its advantages:

First: Protocol (WEP), one of the oldest protocols used in wireless networks encryption, but it suffers from a big weak spot, registered any penetrative professional breaking this protocol over a short period, and are advised to use protocol (WEP) with key length of 128 bits, because it provides protection better than the shorter 64-bit key, and the key is created in the access point can then be copied to any device that is connected to the wireless network, and called this kind of common key encryption key (PSK).

Second Protocol (WPA) is the best protocol of the previous protocol, which provides the strongest encryption level, and often access and calling cards in the devices available in the market points of support over the past three years of this Protocol, and the availability of new operating systems support for the use (WPA), and can be used with an encryption key is shared (PSK) and with the encryption algorithm (TKIP), in Windows XP called Protocol (WPA - PSK), where should the user to copy the encryption key for the device to be connected to the wireless network, and can be used on a larger scale in institutions using Documentation / EAP 802.1 and in which the use of electronic certification mechanism.

Third Protocol (WPA2) which is an enhanced protocol (WPA) features that uses AES algorithm for encryption, it is also used in the bilateral networks, ad-hoc, and is available in a way (PSK) or using documentation / EAP 802.1 mechanism during which he can use the electronic certificates.

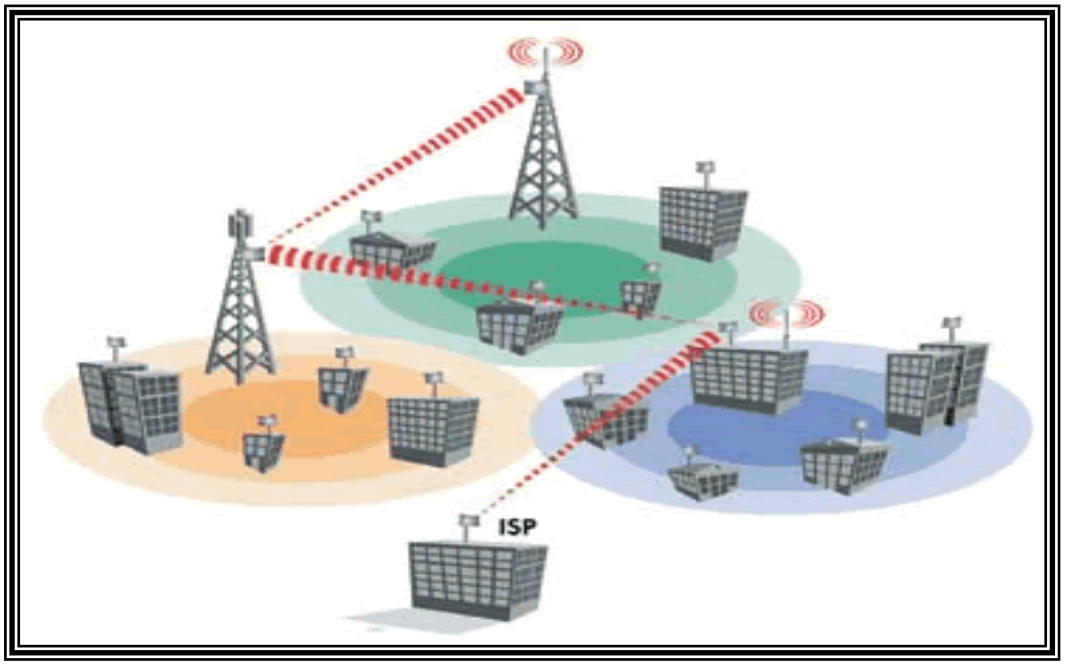

Fig 1: Contact the wireless network

II. WIRELESS NETWORKING PROBLEMS

Piracy operations on wireless networks in the recent period have become very many and varied the discovery of serious piracy operations targeting wireless routers (routers) to conduct malicious those changes, as the number of devices that have been controlled so far to 300 thousand sets of various types, including D-Link, Micro net, Tend, TP-Link, and other network routers. Hackers have resorted to the use of a variety of techniques that helped them access to these devices and make changes on the DNS system which is used to translate domain addresses and routed to the IP device user address of the computer to determine the device-specific Web servers, according to the published report pointed out last Monday by researchers at security firm Team Cymru.

This allows the penetration process to hackers planted a blank password in the wireless routers for users of type TP-Link words, in addition to the other way allows them to control the passwords for wireless network WPA / WPA2 remotely, So far, these attacks, involving more than 300 thousand sets in a wide range of countries, include India, Italy, Thailand, Colombia, and Vietnam. The ultimate goal of this process is to redirect end users to malicious sites trying to steal your bank accounts passwords.

It is clear that there are weak points in the direction and the modem and other devices that rely on its own internal operating system devices, it is necessary to fill these gaps exposed millions of users at risk.

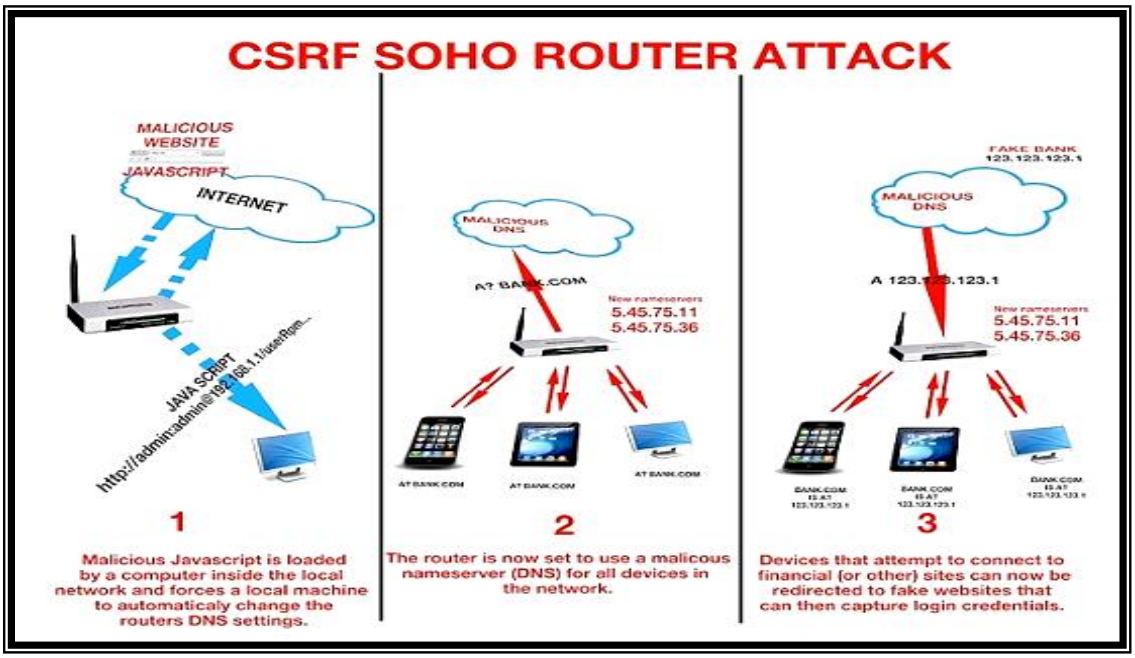

Fig 2: piracy aimed at wireless routers (routers)

III. PROTECTION FOR WIRELESS NETWORK

Researcher explains a number of actions that should be applied to protect wireless networks are summarized below:

1. must be protected access as a user point and password are brought in whenever the user wants to change the settings of the access point, it should be noted that the new access points (or which has been to restore the default by the settings) be password-protected recognizable by the manufacturer, so be on the initiative to change the user password in order to avoid hackers to enter a network and controlled by changing the settings of the access point, and in general should the user choose the appropriate password consists of at least seven boxes to be a mixture of letters and numbers.

2. The most important protection methods are concentrated in the wireless network is encrypted, and there is more than one system (or so-called encryption protocol), a different protection force.

3. must wireless network ID change (SSID) so that does not imply access point type or her whereabouts, the default in new access points indicating the access and manufacturer her point type, allowing hackers an opportunity to attack the access and control points, taking advantage of the special gaps, You should also disable the announcement of the access point identifier option (Broadcasting SSID).

Researcher also adds steps to protect your wireless network:

1. Encrypt wireless network.

This step is the most important action taken to protect the wireless network. Used encryption means today is (WPA2) and (WPA-PSK) and (WEP). Without that go deeper in the encryption techniques (WPA2) is the latest in the world of encryption cry very favourite to buy Router supports this technique. By this encryption can be used for complex password consisting of 64 box (large and small letters, numbers, signs) and recommend everyone to exploit all available fields at secret word set. But how you will remember the pin number composed of 64 boxes? There is no need to write a PIN every time you want to enter the wireless network because it will remain preserved in the network settings, but preferred to write a PIN number on file Txt and keep it on an external USB memory card. Older routers used type of encryption technology (WPA) Note that the previous encryption (WPA2) better than him. For encryption (WEP) never think about using it because it is considered a weak encryption and can penetrate the network within 4 hours (maybe a few minutes) using special software.

2- Use the MAC Filtering

On each network card there is a special code called Pal Mac Address distinguishes it from other network card. I picked up a picture of your network card so you can see the Mac Address. In the router settings you can adjust most settings, so that this does not fall on the wireless network, but according to a specific list of Mac Address.

The researcher recommends some tips to protect:

1-Use a firewall Firewall software on your mobile device.

2- Free hot contact points are often less secured than that paid. Points are paid to follow-up and protection of process and change all safety requirements have with encryption.

3- Turn off file sharing feature on the device to prevent the arrival of any person to own your files or even open the field to participate to do so, remove the property from the files in the Tools menu Folder Options.

4- If in your private and important files then tightly closed with a password. How easy Compress the files you want protected and in the options you'll find a special option put a password for the file even though the person taking the file from your computer will not be able slot and always use a password consisting of numbers, letters and punctuation and a low of eight characters it difficult to decrypt.

5-There are also programs you place after the files and folders words and also programs. To limit their use.

6- Turn off the wireless network card on your mobile device. It has not been operating mode button on the mobile device messes. But he was placed in order to close it after the completion of use. This will save you a first energy and will prevent other people from entering or even access to your device.

7-If you are working on a wireless network card remove the card from Mahmul.albages some tips to protect:

8- Do not connect to a wireless network and your device does not contain a virus protection program. Once you connect to the wireless network there is the possibility that either infected with HIV or electronic worm within 15 seconds if your computer did not contain the anti-virus software modern

IV. CONCLUSIONS

Due to the privacy of wireless networks, the security risks faced by the different from those that exist in Ethernet networks and may be the wireless network is breached gate to the wired network due to the easy access to him. Where is the Access Point of exotic or alien computers (Rogue access point and Rogue Clients) is the security breach is common in wireless networks and this hack is happening as a result of the existence of these devices into the wireless network signal, allowing it to pick up its signal.

REFERENCES

[**1**] Kelley, D. (2003). The X factor: 802.1 xs may be just what you need to stop intruders From accessing your network. Information Security, 6(8), 60-69.

[**2**] Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).

[**3**] McDougall, P. (2004, March 25). Laptop theft puts GMAC customers' data at risk. Information Week Security Pipeline.

[**4**] Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.

[**5**] Kevin Beaver, Peter T. Davis, Devin K. Akin. *Hacking Wireless Networks for Dummies*. Retrieved 2009-02-09.

BIOGRAPHY

Dr. Yasser Elmalik Ahmed Seleman, Sudane

- PhD in Computer Science (Excellent) - Omdurman Islamic University - Sudan.
- M.Sc. In Information Technology - University of Newcastle- USA.
- M.Sc. In Information Technology - TheNational Ribat University .