# PROTECTING WIRELESS NETWORKS FROM VULNERABILITIES, THREATS AND ATTACKS

By

**Bashir Alhaji Bala**
*Department of Computer Science,*
*School of Science Education,*
*Federal College of Education (Technical),*
*Potiskum.*

and

**Alhaji Idi Babate**
*Department of Computer Science,*
*School of Science Education,*
*Federal College of Education (Technical),*
*Potiskum.*

## Abstract

*This paper focuses on the protection of wireless network from vulnerabilities, threats, attacks, configuration and security policy weaknesses. The paper outlined some security policies for an organization; a skeleton policy which helps managers and IT stakeholders to comprehend and evaluate the different threats associated with the utilization of network technology. The paper also discusses the network security weaknesses in router and firewall configured in wireless network devices, types of vulnerabilities and responses to those threats, and the counter measures taken to stop the attackers from getting control of a wireless network. Recommendation on precautionary steps to be followed in order to ensure standards of the security of a wireless network was also highlighted, so as to maintain Integrity, confidentiality, and availability of the wireless network security.*

Security has become a major challenge in the world with Network threats growing rapidly because of the use of personal computers and advances in technology. The National Institute of Standards and Technology (NIST) Computer security handbook defines Computer Security as “The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information resources (includes hardware, software, firmware, information/data’s and telecommunications)”

A security policy is a principle of action adopted or proposed by a government, which determine how an organization treats computational resources. Security should be officially recognised as a critical business objective just like any other important business objective. To ensure security across organization and to assure customers that the company can be trusted, overall security policies must be implemented to include several component policies and procedures that govern how the organisation uses computer networks, protects and distributes data, and offer services to customers. Each component of the security policy defines specific security best practice for a particular topic such as a password policy. These policies and procedures include rules on company internet usage, customer data privacy, company structure, and human resources hiring and termination practices.

Network security is the procedure by which digital information possessions are secured. The objectives of security are to ensure secrecy, support integrity, and guarantee accessibility. In view of this, it is basic that all networks be ensured from threats and vulnerabilities in place for a business to realize its fullest potential. Regularly, these threats are diligent because of vulnerabilities, which can come up from misconfigured hardware or software, poor system outline, inherent innovation shortcomings, or end-client indiscretion. A router is comparable to numerous computers in that it has numerous services empowered by default. A number of these services are unnecessary and may be utilized by an attacker for data assembling or for abuse. All unnecessary administrations should be disabled in the router configuration to counteract the attacker from utilizing it to harm the network or to take the essential data, or network units' configuration (Alabady, 2009).

**Wireless Network**

A wireless network is a computer network that is not connected by cables of any type. The network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. Wireless networks consist of three basic components: the transmitter which transmits radio frequencies; Access points that provide a connection to the organizational network and/or the client devices (laptops, PDAs, etc.); and the users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability (Choi, Robles, Hong, & Kimi, 2008).

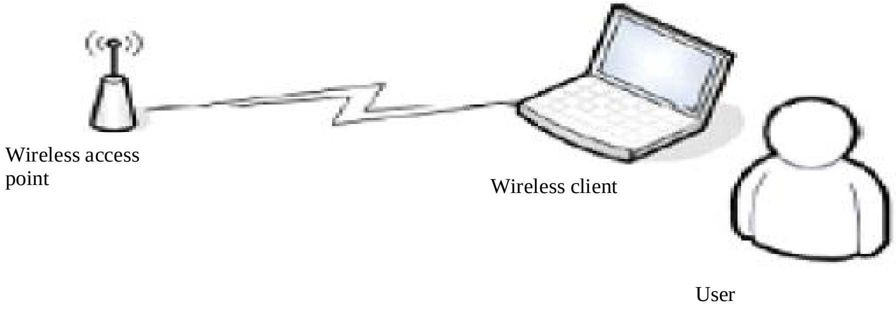

**Figure 1: Component of a Wireless Network**
(Source: Choi et al. 2008)

### Security of the Wireless Networks

The security risks presented by these networks include insertion and interception attacks. In the insertion attacks, a system cracker inserts an access point or client into a network for the purpose of inserting unauthorized packets into the data stream. In case of the interception attacks, a system cracker intercepts message traffic. The sniffed packets are then subjected to analysis that will break weak encryption keys (Ron, Zhao, Yan, Cayirci & Cheng. 2013).

### Wireless Network Security Threats

Wireless networks are susceptible and exposed to attack because of its borderless nature. The reports published by NIST Computer security handbook (NIST, 2002), describes attacks on 802.11 wireless networks that expose organizations to security risks as attacks on confidentiality, integrity, and network availability. Figure 2 below provides a general taxonomy attacks to help organizations and users understand some of the attacks against WLANs.

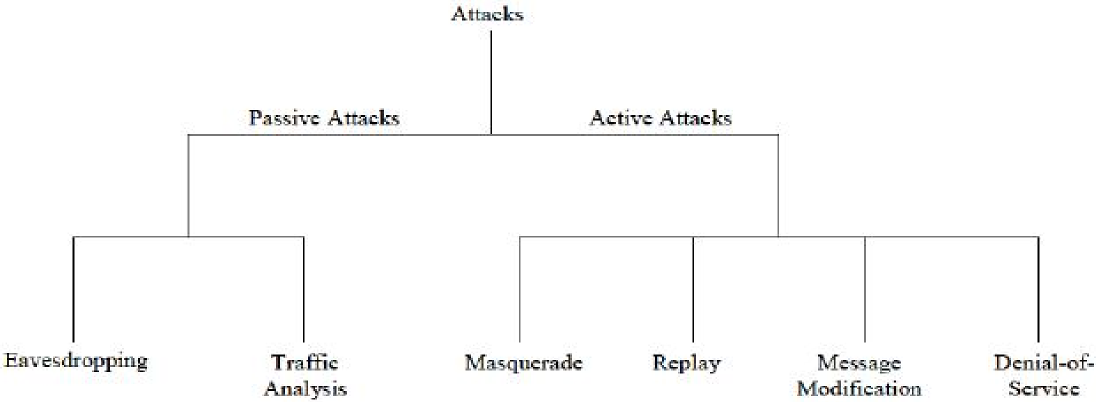

**Figure 2: Taxonomy of wireless Network Security Attacks**
(Source: NIST, 2002)

Figure 2 above shows that the network security attacks are divided into passive and active attacks. These two broad classes are then subdivided into other types of attacks as shown in the diagram.

1. **Passive Attack:** An attack in which an unauthorized party gains access to an asset and does not modify its content. Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis).

i**.** **Eavesdropping:** The attacker monitors transmissions for message content (NIST, 2002; Stallings, 2013). An example of this attack is a person listening into the transmissions of a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

ii. **Traffic analysis:** The attacker in a more subtle way gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties (NIST, 2002; Stallings, 2013)

2. **Active Attack:** An attack whereby an unauthorized party makes modifications to a message, data stream or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types: masquerading, replay, message modification and denial-of-service (DOS) (NIST, 2002, Stallings, 2013).

i. **Masquerading:** The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

ii. **Replay:** The attacker monitors transmissions (Passive attack) and retransmits messages as the legitimate user.

iii. **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing or reordering it.

iv. **Denial-of-service:** The attacker prevents or prohibits the normal use or management of communication facilities. Attackers launches Denial of Service attack by replaying packers in order to generate noise or by sending de-authenticate packets to the legitimate users in the subnet (Stallings, 2013). In fact, according to Belly Rachdianto (2012), this is the technique used by a large group of hackers. “Anonymous’ to bring down governments web serves in the recent attacks.

The risks associated with 802.11 are the result of one or more of these attacks. The consequences of these attacks include, but are not limited to loss proprietary information, legal and recovery costs, tarnished image and loss of network service.

**Threats Detection Tools**

Vulnerabilities and exposures in most situations are because of poor system management, patches not installed on time, weak password policy and poor access control. The following are the major threats detection tools.

**Wireless Scanners and Sniffers:** Wireless sniffers and scanners capture and diagnose WLAN packets from the air by monitoring the airwaves for all WLAN movement. They detect most Aps and dynamic wireless stations within range. They can also furnish detailed information about the configuration and security utilized by each device (Motorola, 2011)

**Wireless Traffic Injection:** It depends on a wireless device to inject a special frame over the air. In the event that a sniffer sees an unapproved AP, it tries to connect with it wirelessly and consequently inject a frame that could be followed on the wired-side by a server or by an alternate sniffer joined on the wired-side. While this technique works with rogue Aps that have inherent routers, it comes up short if the rogue AP has security empowered. Provided that security is empowered, the sniffer won't interface with the apparatus. Furthermore, this technique uncovered the wireless IPS system by driving it to transmit outlines over the air in an effort to locate rogues (Motorola, 2011).

**The Motorola Air Defence Solution:** Air defense distinguishes all WLAN devices, which incorporate Aps, WLAN user stations, virtual Wi-Fi, and distinguishing offering devices such as printers, wireless bar code scanners for sending or stock requisitions, and so forth. Air defense additionally recognizes rogue conduct from ad-hoc or peer-to-peer networking between user stations and coincidental acquaintanceships from user stations interfacing with neighbouring systems. Motorola Air defense can protect against wireless threats by means of the air by ending the wireless association between any rogue device and an authorized device using Air defense patented techniques (Motorola, 2011)

**Securing the Security of a Wireless Network**
Everybody is exposed to threats in wireless network as no network is fully guaranteed as secured. Hence, network administrators and users must be more serious in curbing security issues in wireless networks and apply countermeasures to lessen the risks of security issues. Here are some practical recommendations for countermeasures to the threats in wireless networks (Noor & Hassan 2013).

**Change the Default Service Set Identifier (SSID):** Since the default SSID is also used as the password to the network, so also the need to change the default SSID value, because an attacker might assume the network is badly configured.

**Turn on the Encryption:** It is recommended to use encryption on the wireless network; be it WEP or WEP/2, encryption must be enabled. Encrypting wireless network is by far better than leaving it as an open network. No network is ensured secured, however at any rate safety measures might be taken with the goal that the attack is less inclined to happen and more challenging to launch. Henceforth stronger algorithm such as CCMP is recommended for the encryption (Loshin, 2013).

**Disable SSID Broadcast:** By broadcasting the SSID into the air, it signifies the presence of the network without any exertion. It is like alerting hackers to penetrate into the network.
Broadcasting the SSID should be strictly discouraged.

**Policy Enforcement:** In order to handle threats that may arise on account of social engineering, there is a need for a well comprehensive agreed policy between employees and employers which must be strictly adhered to as a rule.

**Disable the Wi-Fi Adapter:** This is important to stop auto connection from the malicious access point in the network. It is likewise important to dependably monitor the access point that will connect to the Pc by configuring the network setting.

**Secure Your Confidentialities:** Encrypting and setting privacy to important folders as well as disabling file sharing are safety measures toward utilising public WiFi.

**Efficient Devices Management, Control and Monitoring:** A secured network may as well have all the Aps to be enrolled and an automated system must be sent to empower Aps updating exercises. Role Based Access Control (RBAC) is a system that will dole out a function to existing devices dependent upon how they were authenticated. RBAC defines devices accessibility level and what they can access from a network. In order to avoid misuse and abuse of the network and other security breach, a secured wireless network management should be able to monitor users' activity in real time. This is important as there will be hundreds or thousands of devices connected to the network, so it is important to monitor and manage the applications and programs that they are using in the network.

**Packet-filtering Firewalls:** Filtering a network reduces the possibility of users spreading virus. A Packet Filtering firewalls is typically actualized by configuring a router to channel packets going in to both bearings. A packet filtering router generally can filter (i.e. block) IP packets dependent upon some or the greater part of the accompanying fields: Source IP address, Destination IP address, TCP/UDP source port, and TCP/UDP destination port (Pandy, 2011).

**Proper Network Segmentation and Segregation:** A secured network might as well have clear and strong boundries of wireless network that could be accessed by the users. Evaluate the way that the network firewall and IDS devices handle fragmented IP packets by utilizing **Fragtest** and **Fragroute** when performing scanning and examining activities.

**Wireless Network Auditing:** To visualise what is really happening in the network, in order to be proactive and work smarter, the network needs to be regularly audited for all access points and WLAN nodes. This is to stop the attacker from injecting bogus packets. Commonly available network mapping tools like netsnumbler and wavelan-tool can be employed. Specialized tools such as Airsnort can be used for auditing weak keys such as WEB cracking (Choi et al. 2008).

**Training and Educating Users:** Effective networking policy trainings on secure wireless behaviour and on new challenges should be planned and developed through interactive materials to end users. As in the case of Figure 1, users are the fourth component of a wireless networking environment (Choi et al 2008). Training is the only available tools that provide easier and comprehensive understanding of the Network operations. Principally, standards can only be maintained if clients understand the rules and policy to be followed.

## Conclusion

This paper presented facts that wireless networks are susceptible to attacks and prone to many types of threats. This is due to its design, configuration and popularity. Although it is impossible to completely eradicate all risks associated with wireless network, but it is possible to achieve a reasonable degree of overall security by adopting countermeasures such as encryption, packet filtering and firewall techniques. Adhering to the tips and recommendation will ensure the security of the network against attacks from vulnerabilities and threats. There are different definitions and ideas for the security and risk measures from the perspective of different persons. First, an organization should know that it needs security on the level of the organizational set up. Security policies should be designed first before their implementation, so that future alteration and adoption can be acceptable and easily manageable. Finally, the paper concludes by emphasizing the important of training and educating users intermittently, and this will energize the viability of policy organizational wide knowledge and consistence; all in an effort to ensure the integrity, confidentiality, and availability of the security of a wireless network standard. Conclusively, Standards won't be followed if nobody knows they exist.

## Recommendations

Most organizations use Ethernet network, as a matter of fact security policy to be adopted are as follows:

1. All users in the organization should only have Read access right but no Write access. That is, users should not have installation right to their computers. Only the system or network administrator should have that privilege to make installation for all the users in the organization so as to avoid malicious software's (malwares). Malwares can give a remote hacker access to penetrate a computer on the network using backdoor method so as to steal or damage information on that computer. This will solve the problem of integrity and confidentiality in network security.

2. Every software update should only be performed and controlled by the file server and the system administrator using the software push method to all hosts (computers) on the network. This will bring about installation of genuine, reliable and authentic sources and installation of software's free from malwares.

3. The file server (i.e. the computer file server), the Ethernet network cables, network Rack, switches, routers (including wireless routers) and all the network equipment should only be accessible by a network expert and to be made out of bounds to all users except the network administrators. This will solve the problem of an insider attacking the network or causing the problem of network availability which is one of the four security challenges of network and computer.

4. Since the organization also has wireless network, the coverage of the network should be minimized or limited to within the organization. That is the network coverage should not cover more than the organizations building area.

5. A strong password should be used for accessing the wireless network. This will prevent the over flooding of the network. It will also prevent intruders and hackers from accessing the network to cause problems to the network security.

6. Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centres, and people who require their data to be hosted buy or lease storage capacity from them. Since it is a third party organization that host the data of an organization, then there should be a security policy agreement between the organization and the cloud storage organization and those policies must be based on, data integrity, confidentiality and availability.

7. It is vital to educate and create awareness to employees in the information technology security field for the establishment of security policies and guidelines for their development process (GAO, 2013).

8. Continuous testing and evaluating the capability and effectiveness of technical security control measures applied for IT systems and networks should be carried out. (MIT, 2011).

## References

Alabady, S. (2009) Design and Implementation of a Network Security Model for Cooperative Network, *International Arab Journal of e-Technology*, 1(2) 26-36, Online, available at: http://core.kmi.open.ac.uk/display/918981 (Accessed: 07/10/2013)

Choi, M., Robles, R.J., Hong, C., & Kimi, T. (2008) Wireless Network Security: Vulnerabilities, Threats and Countermeasures, *International Journal of Multimedia and Ubiquitous Engineering* 3(3) 77-86.

Chris McNab, *Network Security Assessment: Know Your Network,* Second Edition, O'Reilly, 2007, ISBN: 0-596-51030-6.

GAO-013-0546 (2013). *Information Security Agencies Continue to report progress but need to mitigate persistent weakness.* April, 2013.Available at: http://blog.govsellingsolutions.com/author/lbbristow/page/2/: (Accessed: 10/10/1013)

MIT, 2011. National Cyber security policy. [Pdf] INDIA: Ministry of Communication and information Technology. Available at http://mit.gov.in/sites/upload_files /dit/files/

Motorola, 2011. Tired of Rogues? Solutions for Detecting and Eliminating Rogues Wireless Network, White paper Motorola Inc. 1303 E. Algonquin Road Schuamburg, lllinois 60196 U.S.A October, 2011, Online available at: http://www.motorolasolutions.com/web/Business/Products/Software%20and%20 Applications/Network%20Design%20Software/AirDefense_Security_Complianc e/_documents/Static_files/Tired_of_Rogues.pdf (Accessed: 18/10/2013)

NIST, (2002). Wireless Network Security 802.11, Bluetooth and Handheld Devices, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, U.S. Department of Commerce NIST Special publication MD 20899-8930, November, 2002.

Noor, M. M. & Hassan, W. H. (2013) Wireless Networks: Developments, Threats and Countermeasures, *International Journal of Digital Information and Wireless Communications The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2225-658X) pp.119-134*

Pandey, S. (2011). Modern network security: Issues and challenges. *International Journal of Engineering Science and Technology*, May 2011 ISSN: 0975-5462 3(5) 4351- 4357. Retrieved from http://www.ijest.info/ (Accessed: 21/10/2013)

Rong, C., Zhao, G., Yan, L., Cayirci, E., and Cheng, H. (2013) Wireless Network Security *Computer and Information Security Handbook (Second Edition), 2013, pp 285-300*