ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 12 , December 2016

# Attacks on Wireless Networks

**DVSS.Suubrahmanyam**

Dept. of CSE, Swami Vivekananda Institute of Technology (SVIT), Secunderabad-500003, Telangana

**ABSTRACT:** The domain of wireless communications has become a centre point of entire communications networks. All network users are converting into wireless communications networks because of the features and advantages offered by wireless communication networks. As the demand for wireless communications increases the demand for Wi-Fi devices are also increasing proportionately. Wi-Fi is a network technology which has been an in-built feature of many Wi-Fi devices. As the demand for Wi-Fi devices increases the threat to security features are also increasing rapidly. Levels and intensity of securities differ from device to device. No two types of Wi-Fi devices have same security features. This loop hole opens the door for attacks on wireless networks. Hackers are utilizing these negative points for their anti-social activities.

**KEYWORDS:** wireless communications, Wi-Fi devices, security threats, Denial of Service

## I.INTRODUCTION

Wireless communications are based on wireless networks. Wirelee Fidility (Wi-Fi) is a networking technology that enables computer desktops, laptops and electronic devices to communicate each other over a wireless network environment[2][3]. Some specific electronic devices are needed to connect computers, laptops and other devices to wireless network and these devices are called Wi-Fi devices. As the market for wireless communications is growing the need for Wi-Fi devices is also increasing accordingly. Users are purchasing millions of Wi-Fi devices every year as per the statistics given by Government of India [2]. Usera are purchasing these devices and making them connected to wireless networks. But users are not taking the issues created by these devices into consideration [3][4]. Various security measures are to be set up on these devices. Users are not considering them as an important steps thaa they have to follow. Security measures differ from device to device. Improper or negligence installation of security measures on these Wi-Fi devices are prone to many security threats and security attacks on users because of descrepencies among Wi-Fi devices in terms of setting up their security features [2][3][4]..Thease differences allow hackers to enter inti computer systems without knowledge of users.and attacking their systems. In this paper the reasons of security attacks, the way of attacks , pre-caution measures to be taken to avoid them etc., are discussed. The basic function of Wi-Fi devices is to enable electronic devices to connect to internet. Once sources of security threats and security attacks are known then prevention can be made easily [1][2][3][4]. This is the main out put of this paper.

## II. ATTACKS IN Wi-Fi ENVIRONMENT

Firstly, users have to know how attacks are occured in Wi-Fi environment. Transmission Conntrol Protocol / Internet Protocol (TCP/IP) is a set of communication protocols used to interconnect network devices over an internet [2][3][4]. TCP/IP implements layers of protocol stacks and each layer provides and supports a well-defined network services to its upper layer. Physical layer is one of the layers of TCP/IP model through which wireless access points are being operated. Thus all access points are operated in this physical layer. Hackers exactly concentrate on these access points. Hackers introduce an electronic device on the path of access points which produces noise with the same frequency band in which wireless access points are operated. Then this noice mingles with the existing bandwidth and disallows to connect to its desired point. Thus users can't reach their desired access point. As a result users will get Denial of Service (DoS) message [2]. Then hackers put an unauthorized access point to make attacks on users. This is the way how attacks are occuring.

Secondly, there another way of Denial of Service (DoS) attack on users. In general no problems araise btween two wireless communications. But when a wireless user sends data to a wired user, real problem happens. In general, wireless communication reaches to a wired communication through an access point [2][4]. To connect to a particular access point , users need to have Service Set Identifier called SSID. Hackers always try to place an authorized access point with the same SSID. Then whatever data user sent to a particular access point will be received by an unauthorized access point which is maintained by hackers. Then hackers use the valuable data what they received and enters into the system by cracking Wired Equivalent Privacy (WEP). They create an abnormal traffic in the network which may lead to Denial of Service (DoS).

## III. TYPES OF ATTACKS IN WIRELESS ENVIRONMENT

Attacks in wireless environment can broadly be categorised into 3 major groups [2]. 1. Denial of Service Attack (DoS) which is discussed above in part II under attacks in Wi-Fi environment. 2. Man-in-Middle Attack in Wi-Fi devices 3. WarDriving

### A . DENIAL OF SERVICE ( DoS ) ATTACK

This attack does not allow users to reach their respective access points. This attack can be applied in many ways. The clear ways of attacking DoS are clearly discussed in the above heading III.

### B . MAN – IN - MIDDLE ATTACKS

It is most commonly applied attack on users. This is also an easy way of attacking wireless network users. This attack occurs in mostly in wireless environment only [4][3]. When wireless user sends any data to an access point , during the transmission another person like hackers can easily collect the data before the transmission packets reach the required access point [3][4]. The way the transmission packets are collected in an improper way without any authorisation is known as Eavesdropping. This method provides a lot of opportunity to middle man to manipulate data in whatever way they want and they use the same dadta for their personal benefits. In this method users privacy is denied without their authorisation . So usera are advised, always, to use strong encryption methods for their data.

Strong encryption methods can't allow the data packets to be broken easily even though they are Eavesdropped. Mostly hackers use to employ this method for attacks. The affect of these types of attacks has a little impact in case of wired network communications as data transmits only through cabled wire which , in general, does not give any chance to middle man to enter into its transmission path. So regarding Man – in – Middle attacks are cocerned wired networks are very safe comparing to wireless networks [2][4].

### C . WARDRIVING

It is a method of identifying Wi-Fi spots i.e., access points located at a particular desired place. Hackers always move with a device at a particular location where they wanted to make security attacks on users. They move around the location with a device which identifies Wi-Fi access points of users. Hackers employ this method particularly because they can utilise access points without any encryptions as these access spots do not need use any encryptions. If any users using these access points will very easily be attacked by hackers. So users have to care of this important attack . It is always better not to use access points in unauthirized places [2][3][4].

## IV. WI-FI NETWORKS IN PUBLIC PLACES

The main disadvantage of wireless communication is that any person can connect to an access point within the rangr of tat access point if it is not secured. Users sare advised not to use any unauthorized access points in public places. So any user with Wi-Fi connectivity in its device can be connected to unsecured access points very easily in public places . Hackers always try to establish unauthorized access points to get connect themselfs to users. Once connection is established by hacker in users system then entire control of system will go into hackers control. They can do anything by stealing important data from users systems. They can send malicious code into the system, install trojan into the system etc., So it is strongly recommended that never auto – connect to open Wi-Fi networks in public places. These guidelines are given directly by Ministry of Communications , Government of India [2].

## V. SECURITY MEASURES FOR WIRELESS COMMUNICATIONS

The followng pre cautions are advised in addition to the above necessary steps [2][3][4].
1.Users should always use lengthy passwords with a minimum of 15 characters. The degree of complexity and security increases as the length of the password increases. It is very difficult for hackers to break its encryption.
2.Passwords are to be changed frequently, this is strongly recommended for users who perform financial transactions in a wireless network environment. Hackers can't concentrate properly on passwords which are frequently changed.
3.It is always better to shutdown systems or other computer devices when they are not in use.
4. Always use authorized access points 5. Seperate wireless network from wired network by employing strong firewall and anti –virus.
5. Always allow access points which are based on MAC (Media Access Contoll) address .If it is followed properly then most of the security attacks can be avoided easily.
6. Use strong firmware is needed to maintain access points.
7. Service Set Identifier (SSID) is used to identify the location of access points on the networks. SSID provides name of the network users. So the name of the network is not to be publicized. This is not needed for home users.

## VI. CONCLUSION

Users should aware of different types of security threats on wireless networks. Generally users do not pay much attention on security issues attached to their devices. This is the reason why security attacks are taking place. These security attacks incur huge losses and damage to the public and Government as well. So users are requested please do not take them as an easy one and every one should know about all these security attacks and threats and they should make others aware of all these important things. It is necessitated because Government has been working on the lines of Digitalization in which every citizen has to participate and contribute its efforts to the Nation [2].

## REFERENCES

[1] Chris Anley, The Shell Coder's Handbook, John Wiley & Sons page no. 18 – 65, 2011
[2 ]Information Security Education & Awareness , Department of Electronics & Information Technology, Ministry of Communications & Information Technology, Government of India
[3] Jon Ericson, Hacking The Art of Exploitation, Starch Press , 2 nd edition page no. 98-126 , 2008
[4] Kevin D Mitrick, The art of Intrusion , Computer Security Books, page no. 86-125 , 2005

## AUTHOR 'S BIOGRAPHY

Dr. D.V.S.S.Subrahmanyam is a Professor at Dept. of Computer Science & Engineering at Swami Vivekananda Institute of Technology (SVIT), Secunderabad. He did his graduation AMIETE, M.Tech and Ph.D in Computer Science & Engineering, Also did M.Sc in Industrial Mathematics and another M.Sc in Mathematics and M.Phil in Mathematics. Areas of interest include Software Engineering, Software Quality Analysis, Cyber Security and Big Data Analysis..