Wifi Technology and its Security

Thajudheen Kalathil
Department of MSc(IT)
Jain University ,Bangalore 69,India

Dr.Suchithra. R
Head Of MS(IT) Dept
Jain University ,Bangalore 69,India

***Abstract*:- It is the wireless network which is very fast and reliable way to connect to the internet, It will work on two modes ad hoc and infrastructure. communications through mobiles, computers, laptops, wireless networking technologies have extended to a great level now a days Wireless technology provides the enough benefits like portability and flexibility, increased productivity, and installation costs are very low ,biggest challenge will be the data security,The data is transmitted using radio frequency , any user can connect to the network with the help of the transceiver so it should be properly secured and risk of external threat is high .Wireless technologies have become very popular these days in business as well as in personal lives.**

INTRODUCTION:

Wireless networking technology is well known as Wi-Fi which uses radio waves and provide wireless high-speed internet and the network connection ,the common misconception is that the term Wi-Fi is short for "wireless fidelity," however this was not the case. Wi-Fi is just simply a trademarked term meaning IEEE 802.11x, Wi-Fi doesn't need any physical wired connection to astablish a connection between sender and receiver instead it uses radio frequency (RF) technology, Even after protocols such as IEEE 802.1x and WPA are deployed, corporate networks can be compromised by off-the-shelf 802.11 hardware and software. Wi-Fi is also supported by many devices which includes video game consoles, home networks, PDAs, mobile phones, major operating systems and also most of the applications. Any products that are tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they were from different manufacturers. For example one user with a Wi-Fi Certified product can use any brand of access point with any other brand of the client hardware which is "Wi-Fi Certified",Products that pass this certification are required to carry an identifying seal on their packaging which states "Wi-Fi Certified"

Figure1: Wireless Fidelity Tehnology

WIRELESS NETWORK CHALLENGES:

Rogue access points:
Unknown and unmanaged devices inside the network will become wide-open back doors, it also provides an easy routes for malware that should come in and Information to leave the network. The first thing in countering this problem is to enforce no-wireless zones, ensuring that access points do not appear where they are not allowed[1]

Misconfiguration:
Misconfiguration of switches and access points that still represents a huge problem because wi-fi is a new technology, and its administrators have very less experience than wired networks

UNMANAGED USE OF WIRELESS OUTSIDE THE ENTERPRISE:

A large number of employees are becoming mobile addicted," using devices in and outside, open networks. that can leave them into vulnerable or malicious traffic. That is very true with Windows 7 support for Virtual WiFi, which allows neighbours to share access to a laptop[2]

Hackers:

The Active attacks which is held with wireless links are a very big growing problem because mobile and wireless computing does offer an attractive targets to hackers. when a device becomes powerful enough and if the information that contain becomes valuable enough, then they attract the attention of bad guys and are likely to fall victim to exploits[3]

Integrity:

It is defined as the information not being opened by third person and it should reach in the same format as it was sent by the sending party[4]

ATTACKS ON WI-FI NETWORKS:

Sniffing

A "sniffer" is a device or a program that is used to monitor the data which will pass through a computer network. The information is also examined to determine the type of the data, where it had come from, and where it will go. Sniffers collect a huge amount of information that can then be filtered to look for specific content, such as login credentials, email messages, and various types of documents.

The hackers always use the collected information to first map the network and understand the full operating systems that involved, installed programs, the IP addresses and also network topology. This helps to formulate an attack, although it is not uncommon for credentials or other vital data to end up being sent unencrypted over the wireless network during this probing period,.

The most common method of sniffing which involves the use of the network card operating in "promiscuous mode," which allows to receive all the data passing over a wireless network instead of data sent to the specific MAC (Media Access Control) address assigned to the card. When functioning in this manner the card does not usually send out data, thus making it useful to troubleshooting connectivity problems, but also making it ideal for sniffing attacks.

The best way to protect your network against sniffing attacks is encryption. Encryption makes it so that even if a sniffer is able to collect information there is no way they could read it.

SOCIAL ENGINEERING

The hackers can easy to break the security in network and simply asking for access. By existing user, or a third party who have require legitimate access to a system, login credentials can be stolen, providing access past the normal defences . The wireless networks an attacker could ask another user to borrow the generic login credentials .The employee training is necessary to prevent these types of social engineering exploits.[5]

PROBLEM STATEMENT:

The hackers can easy to hack the Wi-Fi technology . So the security is important for the Wireless technology.

To solve this problem some methods has been proposed as follows.

Proposed Work:

Nowadays People feel very easy to use the internet facility from the Wireless Access Point. For this type of security problem, here in this paper I have proposed mainly two strong securities

- Fidelity Protected Access (WPA).
- Wired Equivalent Privacy (WEP).

Now a days majority of the wireless equipment's comes equally Wired Equivalent Privacy and Wireless Fidelity Protected Access.[6]

(WEP) Wired Equivalent Privacy the most important weak point here is that, it makes use of the static and fixed encryption keys. Consider that if you connect a Wi-Fi Router with a (WEP) encryption key, and this must be utilized with each and every device. Then your system or the particular network will encrypt the packets which it receiving, it will be further transmitted. This WEP is strictly considered to produce a natural security and protection in the wireless communication technique

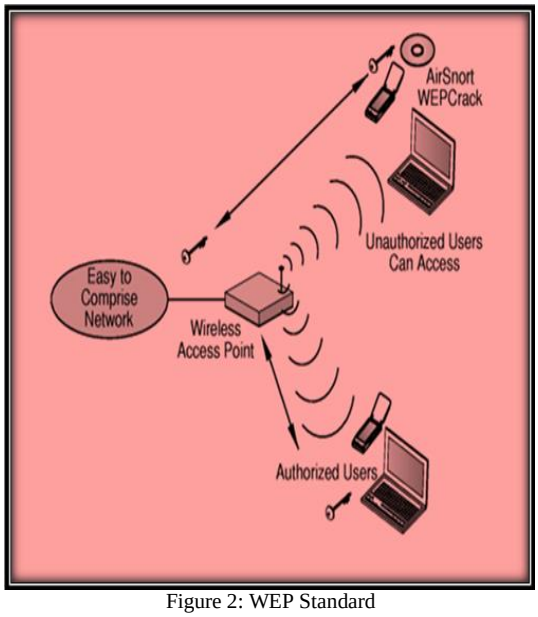

Figure 2: WEP Standard

In the Figure as showing 2, Wired Equivalent Privacy (WEP) for securing wireless networking. The wireless Access Point (AP) is used by both verified and unauthorized user. There for sensible WEP cracking can be

simply verified with some equipment's such as Air crack etc. Air Snort has the excellent capacity to crack the Wired Equivalent Privacy (WEP) weak or pathetic keys.[7]

CONCLUSION:

Wi-Fi is a simple and cost effective way to connect to internet without the need of wires. It is growing in popularity because of decreasing cost and the freedom it gives to users communications through mobiles, computers, laptops, wireless networking technologies have extended to a great level. This does a maximum coverage all over the world. Security issues have also been crossed a level in Wi-Fi network because of the unauthorized users and the Wi-Fi hackers. So to implement the possible Security WEP, WPA, as has been proposed in this paper to overcome the possible security problems.

Through these types of networks and protocols, some of the security problems can be solved. In future, many latest technologies will be initialized

REFERENCE:

[1] http://www.practicallynetworked.com/support/030306wirelesssecurity.htm
[2] https://msdn.microsoft.com/en-us/library/cc875843.aspx
[3] http://www.amazon.in password hacker
[4] Seth Fogie, Cracking Wi-Fi Protected Access (WPA), Part 2 , March 11, 2005, Available online
[5] https://blog.digicert.com/wifi-network-attacks-101/
[6] Seth Fogie, Cracking Wi-Fi Protected Access (WPA), Part 2 , March 11, 2005, Available online: http://www.informit.com/articles/article.asp?p=370636)
[7] J. Walker, Unsafe at Anv Kev Size: An Analysis of the WEP Encapsulation, IEEE Submission. (October, 2000

: