International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

Attacks and Risks in Wireless Network Security

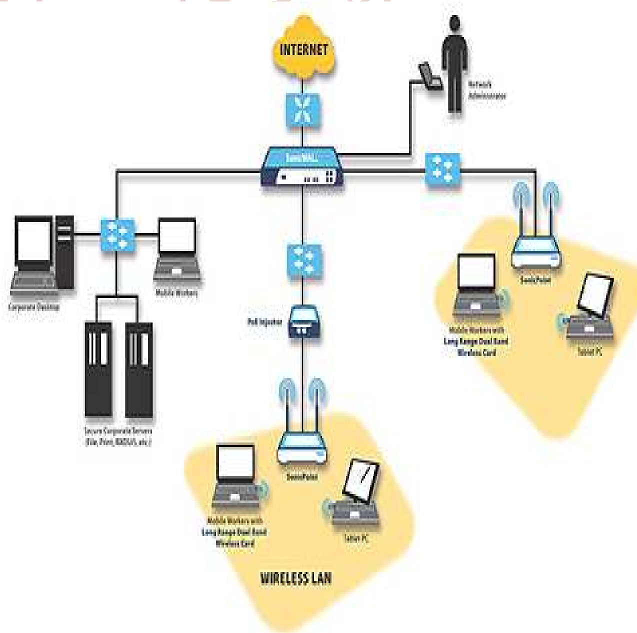
A. C. Sountharraj[1], B. VeeraPandiyan[2]
[1]Assistant Professor, [2]Student
Department of BCA & MSC.SS, Sri Krishna Arts & Science College, Kuniyamuthur, Coimbatore, India

ABSTRACT
Wireless networks are mostly common and are the part of every organisation or an individual. In this article we look into the technology of wireless network and security features of WLANs, delinquent and attacks in IEEE 802.11 WLANs. There are variety of attack methods that can be used against the uses of wireless networks. Modern wireless data network use a variety of techniques to provide obstacles to such attacks. This article also discuss the risks of wireless security in an enterprise. We conclude that combined effort of users, employers and system administrator is required to fight against such malevolent activities.

Keyword: *Network security, risk, WEP key*

INTRODUCTION
Wireless networks became part of every organisation's activity with increase in the use of the internet, it becomes important to keep communications like e-mail, e-commerce transactions and data transmission secure. The reasons are very clear, as wireless technologies comes with huge advantage of being costless, easy to fix up and totally mobile. The use of wireless communication has been around since 1990's mostly used in patented. The obstacles to wireless communication during 90's were many, but these barriers are resolved in these days. There is a huge growth to the use of wireless technology especially in private sectors. The strong advantages of wireless technologies it becomes obvious that business wants to build such a technology. It seems that there are many variety of wireless network technologies in the market, but the one which outstands is WLAN based on 802.11 then we exploit the weaknesses of wireless networks and list the various types of attacks possible on them[1].

TECHNOLOGY OF WIRELES NETWORK:
Wireless communication technology is a modern alternative to traditional wire networking where wired networks relay on cables to connect digital devices together, wireless networks relay on wireless technologies. Wireless technologies are widely used in both home and business computer networks. Low cost device is the foremost reason for wireless technology in acquisition popularity. But such low cost equipment's also facilitates attackers to deploy an attack. And these arrives need to have a secure and well established wireless network in an enterprise.



VULNERABILITIES OF WIRELESS NETWORK:
Vulnerabilities are common for both wired and wireless networks. The attacks on wireless networks that exploit the "over air" characteristics of the wireless signals use the eavesdropping and MITM attacks

Eavesdropping:
Eavesdropping can be described as accidently over hearing a conversation and thus gaining important information which is not easily available.

MITM attacks:
It is known as MAN-IN-THE-MIDDLE attack. The MITM attack is one step beyond the Eavesdropping attack[2]. This is an attack where the person secretly relays and possibly alters the communication between two parties who believe they are directly communicates with each other.

In addition there is the possibility to acquire unauthorized wireless access from a wireless service point. The techniques that can be used are as follows:
- Rogue Access Points
- Rogue Clients
- Open Access Points
- WEP Key Attacks
- Jamming
- High Gain Antennas

Rogue Access Points:
A Rogue Access Points that has been installed on a secure network without explicit authorization from a local network administrator, whether added by a employee or by an attacker.

Rogue Clients:
Enough client is a client that doesn't belong to your company but it is operating on your network anyway.

Open Access Point:
An Access Point is a device such as a wireless router that permits wireless devices to connect to a network.

WEP Key Attacks:
WIRED EQIVALENT PRIVACY is a security algorithm for IEEE 802.11 wireless network

Jamming:
Jamming attacks are saviour denial - of - service attacks against wireless median

High Gain Antennas:
A High Gain Antenna is an antenna with a narrow radio beam that is used to increase signal strength.

SECURITY FEARURES OF WLAN's
The major security services for IEEE802.11 are provided by wired equivalent privacy protocol. As per the IEEE standards there are three basic security features described for wireless networks. They are
- Authentication
- Confidentiality
- Integrity.

Authentication:
A primary goal of WEP (WIRED EQIVALENT PRIVACY) was to provide a security service to check the ID of communicative clients stations. This gives access control to the network by avoiding access to the client station that cannot authenticate properly.

Confidentiality:
Confidentiality, or Privacy, was a second goal of WEP the intent was to prevent information compromise from causal eavesdropping.

Integrity:
Another goal of WEP was a security service created to ensure that messages are not modified in transit wireless clients and access the point in an active attack.

THE RISKS OF WIRELESS SECURITY IN AN ENTERPRISE:
For an enterprise there is lot more than just protecting the network from various attacks. There are different measures enterprise can take, in order to secure their network and the most important one is to keep their wireless access points as safe as possible. The Important reason to keep access points safe is that the attackers do not require specific packing tools as the system itself finds the network when it comes in the range. One of the major risks for an enterprise from their own naïve employees the can contact company databases from a browser and they do the same when the want to work at home. The attackers can take advantages of this and instead of breaking into the security system they would observer the activities of employees and given a chance would get enough knowledge that they can then trick themselves as sincere uses of the enterprise.

Conclusion:
Wireless network security faces a number of hurdles and efforts are being put on, but are relatively new and thus not fully developed. Since wireless technology has huge market but has become almost inexpensive. It is gaining popularity in all sorts of business. These strength of the system security is always countered by its weakest component. So the

end-users must be given proper training on how to secure the data when they are at home or at the private sectors. So that the combined effort of users, employers and system administrators against such malicious activities. Appropriate counter measures can help the organisation to minimise the risk of illegal penetration.

REFERENCES:

1. https://www.researchgate.net/...A.../Wireless-Network-Security-A-filed-Study
2. https://epdf.tips/handbook-of-wireless-local-area-networks-applications-technology-security-and-st.html