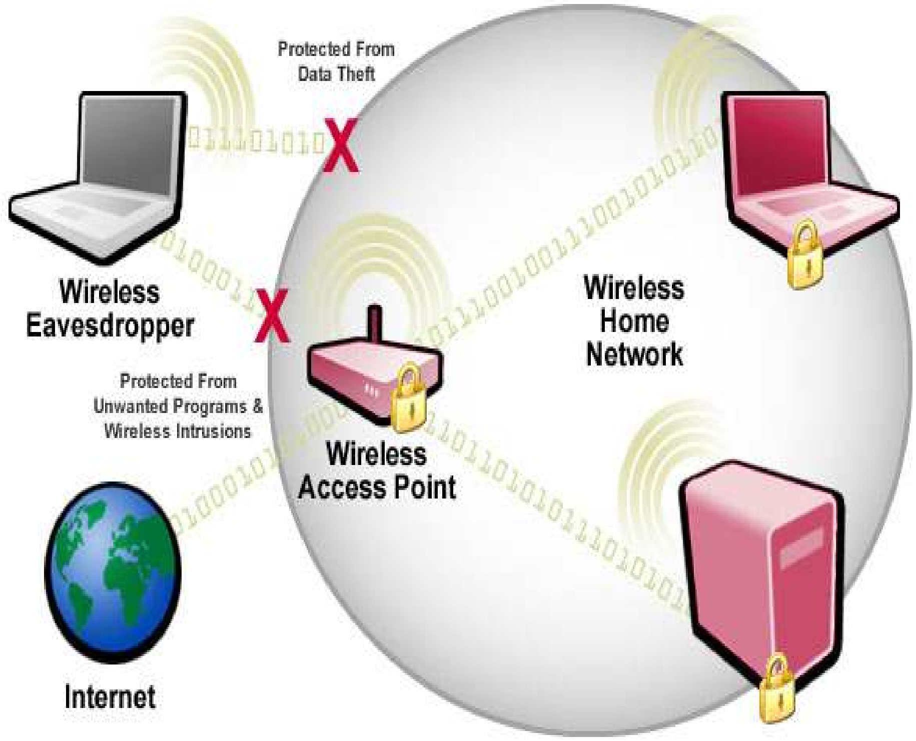
Halmstad University, Sweden

# Security in Wireless Networks

(Report)



**Prepared by:**

| | |
|---|---|
| Mujahid Tabassum | = 830802-T032 |
| Imran Ullah Khan | = 751120-T019 |
| M GulFraz Ayub | = 750310-T052 |

**Subject Title:** Networks Security
**Submission Date:** 13-05-2008
**Submitted To:** Ms Yan Wan

# Abstract

This report will present research on impact of new technologies in the wireless networking field, what are the security issues and how should we need to implement security to reduce the security risk for a secure WLAN environment. The innovation of wireless networking has affected on business and progressively popular due to it flexibility and mobility. This technology has used in every where due to it popularity. Wireless Networking field has developed a lot but it still offers wide area for research in future and it promise to offer more features and functions in the next few years.

The study will converse about wireless networks and indicates the strengths and weaknesses of security in wireless networks and how to enhance the quality of security in different wireless networks. The document will also talk on 802.11 technical standards used into wireless networking.

# Table of Content

# Introduction

Computer is a greatest invention of last century. In today world human life is weary or worthless without computer. Computer's are involved in every field of life and have great impact on human life. It has many applications. Wireless Communication is the one of the greatest application which is used to establish a reliable connection between two or more devices without assisting a wire.

In this age, the emergence of information technology, development of Internet and electronic devices has greatly exaggerated on wireless communication technology. Wireless technologies offer many benefits for user in sense of portability, flexibility, augment in productivity and lower cost. Wireless technologies has great prospect and it covers a wide range of different capabilities oriented toward a different uses and needs. Many kind of electronic devices had been created to implement the experience of wireless technologies such as WLAN, Ad Hoc Networks, Bluetooth, Handheld devices and etc. These devices / technologies offer impressive cost savings and new capabilities to various applications and provides flexible environment for human. The use of these electronic devices / technologies had become daily practice in our daily lives for communication purpose.

Wireless techniques are use to establish a communication medium between two or more devices without a physical link or any hardware (cabling) by utilizing radio frequency. Wireless technology provides great benefits for user but it also can easily break or hack by hacker due to low security. Numerous techniques have been tried, tested and implement based on situation for better security purpose. It can be easily victim of loss of confidentiality, integrity and denial of service from inside or out side of the networks. Unauthorized user access may cause of reduce network bandwidth, corrupted the agency data, and degrade network performance.

Risks are always inherent in any field. Wireless networking raises many security risk issues. There is always need to identify and implement careful security and privacy aspect during implementation of wireless connection. Many kinds of threat and vulnerable can be harass to wireless networks such as

- Malicious entities can gain unauthorized access to user computer and violate the privacy of legal user by follow user work in wireless connection.
- Data could be corrupted during improper synchronization
- User can be affected by malicious entities and these entities can be access to user private document.

In this report we will converse about Wireless devices / Networks, security attacks on networks, attacking tools and how user should implement security issues.

## Wireless Technology:

Today this world has become very advance and many technologies are getting part of our lives. When we talk about wireless networking, it has very wide area and there are so many tools are using for wireless security purposes.

The concept of wireless have developed and started in the array of 19 century by ‘Guglielmo Marconi’. He has created first Wireless Telegraph and Signal Company Limited in 1896 and then in 1901 first wireless distress signal was sent by Morse Code. This technology was prominent during World War II, when it was used for Army activities.

Recently wireless service shows a great development and progress toward new horizon of telecommunication and networking field. Today it has proved a precious and secure communication channel which has been used by almost in any businesses. The first wireless Local Area Network (LAN) was developed in 1971 by emerging of Network Technology with Radio communication Technologies at the University of Hawaii under one of the research project known as ALOHNET. They have implemented wireless networking on bi-directional start topology as experiment [9] [10].

## Wireless Networks:

Wireless networks based on remote information transmission system and electromagnetic waves are implemented on physical layer. Mainly wireless networks can be differentiated into three groups such as Wireless Wide Area Network (WWAN), Wireless Personal Area Network (WPAN), and Wireless Local Area Network (WLAN). It really help user in sense of flexibility and usability, and mobility, WLAN provides a flexible environment for user, in which user can easily move with in wireless networking field without facing the trouble of connection loss. WWAN technology is different from WLAN because it is based on cell cellular network technologies such as UMTS, GPRS, CDMA2000, GSM, Mobitex and HSDPA or 3G. It is basically use for mobile network and cover relatively large geographical area. It provides scalability and huge mobility for user. WPAN technology basically use for personal / home use of interconnection, it has short area distance of 10 meter. The wireless connection between PCs, PDA, peripherals, cell phones, pagers and consumer electronics is considered as WPAN. WPAN know as ‘Plugging In’ because it has flexible security feature. This connection only work under short range, so when two communication devices have come into closer, they can be also connected through cable or Infra Red. WPAN use Code Authentication as an extra security option [4].

### Wireless LAN

WLAN refer to Wireless Local Area Network, in this technology user can connect to network without having the trouble of wire and he can easily move into 100 meter range. User can use all facilities offer within network such as sharing the file, downloading and printing etc. All operation control by one access point device within a WLAN and this access point connected to a wired Ethernet LAN via an RJ-45 port. It provides very flexibility and mobility for user.

Recently, WLAN technology has huge horizon in future and it expanding rapidly, it is due to 802.11 standards. Wi-Fi is mostly use for wireless network and user need to Install

Wi-Fi into his computer and then he can be connect to WLAN. Recently all new Laptop has built in Wi-Fi card [4].

### Ad Hoc Networks

Ad hoc is a Latin phrase and it means is "for this purpose". Basically it offers a common solution for any specific problem. Ad Hoc Networks is a group of different networks such as Bluetooth, cell phone, laptop and PDA etc. These networks are considered as Ad Hoc due to similar architecture and shifting network topologies. The popularity of Small electronic devices and 802.11 / Wi-Fi standards has made Ad Hoc Network very famous. These networks work on a fixed WLAN infrastructure and maintain a random network configuration. In these networks, data flow is controlled by two devices which are connected with each other. Wherever any device will move to any other place, user must need to reconfigure [4].

## Standards:

### IEEE 802.1

Wireless networks use IEEE 802.11 techniques and based on IEEE 802.11 standards. In wireless networks multiple stations are communicate through radio waves with in 2.4 GHZ to 5 GHZ band frequency range. These connections can differentiate into two types. First type known as BSS, where one station acts as master / server, and all other user will be connecting through it. In this case Master station will be responsible for communication and all communication will be passed through it, it work as main Access Point.

Second type is known as IBSS, which is mostly use for Ad Hoc networks. In this case there is no concept of Master and all devices will be connected to each other directly [4].

## Risks and Vulnerabilities in Wireless LANs:

### Insecure wireless LAN Device & Stations

There is a huge difference of security anxiety in wireless and wired networks. In wired network hacker easily can not enter into the networks, because they need to pass-through physical security such as firewall and these networks are protected with in close building. Where as wireless networks air a medium and it is uncontrolled, the signal are travel along walls with in specific range. So it is easy to sniff the traffic instead of wired networks [4].

In wireless technology mostly LAN devices are not vigorous due to their simplicity and flexibility. In some cases wireless access point left insecure due to inappropriate configuration and design flaws, where access points dispatched with default insecure configuration and it will broadcast SSIDs service set identifiers. Then SSIDs will not ask for any authentication, which provide a gateway for hacker to get into the networks. Hacker can used Soft Access Point to act as legitimate user and hack the systems [4].

## Attacks

Accidental Association and Malicious association

Accidental Association attack is kind of unauthorized access to any company or user networks. Basically some time user can simply connect to any Internet source through it wireless connection. He might do not have knowledge of source, is it secure or not. In some cases Hacker or Cracker keep open their network, so when any user will be connect to their network. They can easily enter into their system and steal his personal data. To begin, the hacker sets up a network as a soft access point by using different tools such as HostAP, AirSnarf etc. When victim will connect to this access point, hacker will know victim IP address by giving him free access. Once they know the IP address of victim they can easily steal information, install Trojan horse and other sypware to user system.

Malicious Association attack is kind of unauthorized access but it does not break the VPN, instead of that it takes over the client at layer 2. "Malicious associations are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP)". In this case Hacker creates their own networks which are looks like legitimate, and their access point know as 'Soft AP' [1] [3].

Ad-hoc networks

Ad-hoc networks can easily become victim of hacker. Ad-hoc networks act as peer-to-peer networks between wireless computers and it do not have an access point. Beside this these types of networks has less protection, encryption methods and easily can be victim [1] [3].

Identity theft or MAC spoofing

In this case, hacker or cracker can get access into a network and they can check the traffic on network. By this way they can easily get or know the MAC address of any computer which is work as server or has network privileges. Now a day's wireless system allows the functionality of MAC filtering, this technique only allow authorized computer with specific MAC ID for access. Many kind of sniffing software are used for prevention from Identity theft [1].

Denial of service

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is a process, in which hacker jam any server or system from it functionality by bombing / divert continue traffic on it. It used in different cases, mostly hacker uses this technique to break or slow down the website on Internet or services hosted on high-profile web server such as bank, credit card payment etc. In this technique hacker continues send or bombards packet to any target Access Point until the system will break or become un-useable. Hacker abuse Extensible Authentication Protocol against the authentication server [1] [3].

Brute Force Attack against Access Point Passwords

Some time due to improper knowledge of security user can use a single key or password which is shared with all connection wireless clients. In this technique hacker tries to identify the password by methodically testing of every possible password. The mistake provides opportunity for hacker to trace the password easily and hack the network [1].

### Server Set ID (SSID)

There is always need of server which handle all the traffic and client on the network. SSID is a configurable identification service which offers client to communication with server by using the identical / separate key. These keys can configure manually. Access point come with default SSID, so if these key are not change then networks are easily accessed by hacker. There is always need to reconfigure SSIDs carefully [1].

### Man-in-the-Middle Attacks

It one of the most complicated technique used by hackers. Man-In-The-Middle attack works similar to it name, where hacker act in middle of source and destination as legitimate to break the connection. In this method, hackers break the VPN Virtual Private Network connection between user and access point by inserting a malicious station between of them. This method can simply harm to wireless networks and once a hacker enters into LAN then it hard to recognize him because VPN work on layer 3 while wireless connection exist below the VPN at layer 1 and layer 2. There are many tool uses for this purpose such as DSNIFF, IKEcrack etc. The SoftAP software is use to convert wireless device into a soft access point and it interrupt the communication at middle of session. Then the user will reconnect to hacker access point due to SoftAP software and he will not recognize it, and all the traffic will pass through hacker access point.

There are few solutions for this problem such as user need to use highly capable Intrusion Detection System and 24 hour monitoring tools [1] [3].

### Network injection

In this case hacker can get access to ISP server network system and they make changing in OSPF, RIP or etc protocols. They inject the viruses or bogus into the networks system, which will change the configuration of router, switches and hug. It will make whole network brought down and need to reprogram or reinstall the entire configuration again. So user will lose too much time and energy for re-installment [1] [3].

## Technology / Tools used for Hacking

There are number of tools, which used by hacker over wireless networks, and most of them are freely available on Internet. So there is a competition between IT specialist and hacking specialist.

### Wireless LAN scanner & Sniff Tools

There are number of free tool available on different operating system provide an easy way for hacker to enter into the user network. NetStumbler Probe (Window based) and Kismet (Linux based) are free tools, which are use for searching the access point and broadcast the SSIDs, it provide easy access for hacker to enter into network. These tools are use to monitor and capture the wireless traffic and work through GPS. Hackers use these tools against the user to identify the physical presence of wireless LANs.

War Drives search around cities for wireless LAN signal and post all information one common website (www.wigle.net), hacker use this place to find access point with same SSID and MAC address for any given location.

Antennas

Hacker use high quality and highly range wireless antennas, which help them to capture the wireless signal from long distance. These antennas have ability to receive 802.11 signals from thousand feet away.

To Break WEP Encryption

A number of tools (such as WEPwedgie WEPCrack, WEP Attack and AirSnort etc) used for WEP encryption. It works on WEP encryption algorithm and break the password / authentication by identify the traffic pattern on network.

THC-RUT

It is freeware wireless hacking tools and use for LAN discovery to identify low traffic access point on the networks.

Ethereal

It is freeware wireless hacking tools and use for LAN analyzer to interactively browse capture data and detail information for all observer traffic on networks.

WEPCrack

It is freeware wireless hacking tools and use work as encryption breaker to crack the 802.11 WEP encryption keys.

Airjack

It is wireless network hacking tools and use for Denial-of-Service attack.

IRPAS

It is use to disturb the Internet Routing Protocol services, and cause of attack on routing protocol such as DHCP, IGRP and HSRP.

Ettercap

It is use for Man-In-the-Middle attack. It has functionality of sniffing of live connection and content filtering on the fly.

## Recommendation for Wireless Security

The security on Internet, especially on the wireless networks is very important issue. Risks from crackers are sure to remain with us for any foreseeable future. The challenge for IT personnel will be to keep one step ahead of crackers. There are many hardware and software based tools which are used for security purposes. Company and user need to choice secure and cost effective solution for their networks. The following solutions are very cost effective and secure, for any organization.

There are many technologies use to secure a wireless network from hacker attacks, but currently no method is absolutely secure. The best strategy may be to combine a number of security measures such as:

- All wireless LAN devices need to be secured
- All users of the wireless network need to be educated in wireless network security
- All wireless networks need to be actively monitored for weaknesses and breaches

Firewalls

A firewall is kind of secure and trusted machine which are used between a private and public network. The firewall machines are configured under set of rules or policies to control or manage the different kind of traffic. User has ability to define rules for specific traffic, which should pass or prevent or block. Firewall mostly located inside a corporate network to segregate sensitive areas in an organization. Some firewalls can help to prevent other people from using your computer to attack other computers without your knowledge. Using a firewall is important no matter how you connect to the Internet with a dial-up modem, cable modem, or digital subscriber line (DSL or ADSL) [8].

VPN

VPN stands for Virtual Private Network. VPN gives extremely secure connections between private networks linked through the Internet. It allows remote computers to act as though they were on the same secure, local network. More recently, using the Internet as a means of providing more cost effective access to business critical information such as order status, inventory levels, or even financial information has gained wider acceptance through Virtual Private Networks or VPNs. A Virtual Private Network is a business solution that provides secure, private connections to network applications using a public or "unsecured" medium such as the Internet. With a VPN deployed across the Internet, virtual private connections can be established from almost anywhere in the world [7].

Advantages:

- Allows user to be at home and access company's computers in the same way as if you were sitting at work.
- Almost impossible for someone to interfere with data in the VPN tunnel.
- By using VPN client software on a laptop, user can connect to company from anywhere in the world

There are following VPN-related technologies:

- Connection Manager
- DHCP
- EAP-RADIUS
- IAS
- Name Server Assignment (DNS and WINS)
- NAT

Treat Access Points as Un-trusted

User should treat all access point as un-trusted and he need to identified and evaluated on are regular basis to determine if they need to be quarantined as un-trusted devices before wireless clients can gain access to internal networks. This purpose means appropriate placement of firewalls, virtual private networks (VPN), intrusion detection systems (IDS), and authentication between access point and intranets or the Internet.

### MAC ID filtering

One of possible solution is known as MAC ID filtering. Most wireless access points contain some type of MAC ID filtering that allows the administrator to only permit access to computers that have wireless functionalities that contain certain MAC IDs. This can be helpful; however, it must be remembered that MAC IDs over a network can be faked. Cracking utilities such as SMAC are widely available, and some computer hardware also gives the option in the BIOS to select any desired MAC ID for it's built in network capability [2].

### Static IP addressing

Static IP addressing is also one of the solutions to handle security on wireless networks. User can disable IP Address automatic function of the network's DHCP server, and set the IP address manually. It will make more difficult for a casual or unsophisticated intruder to log onto the network. This is especially effective if the subnet size is also reduced from a standard default setting to what is absolutely necessary and if permitted but unused IP addresses are blocked by the access point's firewall. In this case, where no unused IP addresses are available, a new user can log on without detection using TCP/IP only if he or she stages a successful Man in the Middle Attack using appropriate software [2].

### WEP encryption

WEP stands for Wired Equivalency Privacy. This encryption standard was the original encryption standard for wireless. As its name implies, this standard was intended to make wireless networks as secure as wired networks. WEP comes in different key sizes. The common key lengths are currently 128 and 256 bit. The longer the better as it will increase the difficulty for crackers. WEP protection is better than nothing, though generally not as secure as the more sophisticated WPA-PSK encryption. A big problem is that if a cracker can receive packets on a network, it is only a matter of time until the WEP encryption is cracked [2].

### WPA

WPA stands for Wi-Fi Protected Access (WPA). It is an early version of the 802.11i security standard that was developed by the Wi-Fi Alliance to replace WEP. The TKIP encryption algorithm was developed for WPA to provide improvements to WEP that could be fielded as firmware upgrades to existing 802.11 devices. The WPA profile also provides optional support for the AES-CCMP algorithm that is the preferred algorithm in 802.11i and WPA2. WPA Personal uses a pre-shared Shared Key (PSK) to establish the security using an 8 to 63 character pass-phrase. The PSK may also be entered as a 64 character hexadecimal string. WPA Personal is secure when used with 'good' passphrases or a full 64-character hexadecimal key [2].

Managed Security Services for Wireless

Managed Security Services (MSS) helps organizations establish effective security practices without the overhead of an extensive, in-house solution. MSS providers handle assessment, design, deployment, management and support across a broad range of information security disciplines. This 24/7/365 solution works with the customer to set policy and architecture, plus provides emergency response, if needed. These services help an organization operating wireless networks to:

- Deploy firewalls that separate wireless networks from internal networks or the Internet
- Establish and monitor VPN gateways and VPN wireless clients
- Maintain an intrusion detection system on the wireless network to identify and respond to attacks and misuse before critical digital resource are placed at risk [2].

## Conclusions

Today the world has become very advance and people are use to flexible, affordable devices or environment. Wireless networking field has become very famous among user due to it flexibility, affordability and mobility. Along with the many facilities and cost-saving advantages to wireless LANs, there are also some inherent risks and vulnerabilities. Security issues are always very important in any field. The Internet provides great opportunities to user but it has very bad security issue, many tool has been developing to protect user from lose on Internet. Network security refers to network infrastructure which is created under some restricted policies for different user and it is like a protection of user against outside intrusion. Wireless network security is a process of prevention of unauthorized access or damage or steal of data from outside or within network. So the main goal of network administrator is to protect the user from outside attacks, keep the user data safe and block the unauthorized access of people within a network. Securing a network infrastructure is securing a possible entry point of attacks on a country by deploying appropriate defense. Wireless networks are mostly used to use internet or for communication with in LAN. Different kind of security tools are use for different Wireless Networks and it has different suspects. The hackers, viruses, Internet-based attacks and DoS etc, are an unfortunate fact of life in any form of networking today. Every business and user easily can be victim of hackers. That why, every company / business / user needs to choose right security implementations, which can protect them from these attacks and provide them a reliable platform.

## References

1. Wireless LAN security, URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf, Access Date: 8 May 2008.

2. Wireless LAN security, URL: http://www.scribd.com/doc/2096959/What-Hackers-Know-That-You-Dont, Access Date: 8 May 2008.

3. Security Resource Section, URL: http://www.protexx.com/Default.aspx?tabid=83#Security%20Risks , Access Date: 7 May 2008.

4. Tom Karygiannis and Les Owens, Computer Security, URL: http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf , Access Date: 7 May 2008.

5. What is a WWAN, URL: http://www.wisegeek.com/what-is-a-wwan.htm, Access Date: 7 May 2008.

6. Secure your wireless network, URL: http://www.practicallynetworked.com/support/wireless_secure.htm, Access Date: 8 May 2008.

7. Scott Akrie, Wireless Network Security, URL: http://www.znet.com/fixedwireless/WirelessSecurityWhitePaper.pdf, Access Date: 8 May 2008.

8. Matt Curtin, Introduction to Network Security, URL: http://www.interhack.net/pubs/network-security/, Access Date: 7 May 2008.

9. History of Wireless Network, URL: http://www.jhsph.edu/wireless/history.html, Access Date: 6 May 2008.

10. A history of wireless Technology, URL: http://media.wiley.com/product_data/excerpt/95/04708494/0470849495.pdf, Access Date: 6 May 2008.