

Lecture: #09
Wireless Network Security



Dr. Redhwan M. A. Saad

Head of Cybersecurity Department

Faculty of Informatics

Midocean University



CyberSecurity Fundamentals (CYB670)



Wireless Network Security

Introduction

Wireless LAN
Vulnerabilities

Wireless WAN
Vulnerabilities

IoT Vulnerabilities

Wireless Network
Security Measures

Useful Tips on
Safe Use of
Wireless Network



- **Wireless networks** have got vast grounds in our network communication during the past couple of decades.
- Being comparatively new technology, wireless security is more prone to threats than the wired networks. **Wireless network security** is a part of **computer network security** in which the **wireless access points** and **wireless cards** are used as the points to secure through the latest security protocols, techniques, and algorithms.
- Securing your computers, data, and other digital resources that are connected through wireless connections is commonly referred to as **wireless network security**.
- **Wireless** is a **medium** on which data transfer and computer communication occurs.



- The **protocols** that handle the wireless communication such as **802.11b, 802.11g, 802.11n** and others normally deal with the **physical and data link layers** of the **OSI models**.
- The upper layers of the communication protocols are almost same with a little variation in the modern wireless technologies.
- The protocol stack of 802.11 is shown in the figure.

Internet	Application layer
	Transport layer
	Internet layer
Wireless data communications	Link (MAC) layer
2.4 GHz ISM band radio interface	Physical layer



- It is very important to note that anybody that is in range of the wireless field **can access the signals easily**. That means, your **network is physically exposed to the hackers**. Now, you have to make sure that your network is **logically secure**. Normally, the security of the wireless network starts from the **network layer**, which is third in OSI layer model.
- The use of **MAC address** of the device is also used for the **static configuration of the MAC binding**. But, in other cases, the security of the network takes place at the third layer of the OSI model commonly known as network layer.
- The gravity of the security problems with the wireless networks can easily be assessed from this fact that you **don't need a wire to connect** to the organization network. You can sit in the parking of the company and can have access to **the data layer level of the network**.



- Any wireless network enabled computer connected to the company network through wire can also behave like a point for the hacker to intrude into your network. Thus, the wireless network is more prone to security threats as compared to the wired networks.
- The major threat points vulnerable to security breach in a wireless network include the following:
 - Bluetooth connection
 - ZigBee connection
 - Bluetooth Low Energy BLE
 - Wireless Access Point
 - Wireless Network Cards
 - And others





- The security protocols dealing with the security of the wireless networks are also less mature as compared to those dealing with the wired networks. **The authentication and encryption protocols** are evolving rapidly due to the **increasing use of wireless networks** in our day to day life. The internet of things (IoT) is driving the wireless security market extensively.
- The major data encryption and security **protocols** used by the wireless networks are listed below:
 - Wired Equivalent Privacy (WEP)
 - Wi-Fi Protected Access (WPA)
 - Wi-Fi Protected Access v2 (WPA2)
 - Wi-Fi Protected Access v3 (WPA3)





- Before we deep dive into the security protocols related wireless security and other mechanism used for securing the valuable data and networks from external threats, let's have a look at the major vulnerabilities of a wireless network.
- We explain wireless network vulnerabilities in terms of **LAN and WAN vulnerabilities** in the following topics.
 - **Wireless LAN Vulnerabilities**
 - **Wireless WAN Vulnerabilities**
 - **IoT Vulnerabilities**
 - **Wireless Network Security Measures**
 - **Useful Tips on Safe Use of Wireless Network**



- **Wireless local area network (WLAN)** is more prone to threats as compared to the wired local area network **because wireless network uses open air as the medium**, which is easily **available to anyone located within the range of the wireless radius**.
- A **hacker** can easily connect to the network as far as the medium of communication is concerned. This is a big downside of wireless network as far as the security of the wireless networks is concerned.
- **Like wired network, the wireless networks are prone to the following types of major attacks.**
 - Passive attacks
 - Active attacks



- **In passive attacks** the hackers only try to intrude into the wireless network communication to **steal the information about the network and passwords**. They don't try to damage the digital resources or take any materialist advantages.
- But they take the information, which can be used for **the active attacks** in the future.
- **In passive attacks**, a hacker just listens to the inbound and outbound traffic of the wireless communication. **The main objective of the hacker in passive attack** is just to **gather sensitive information**, which is useful for carryout **active cyberattacks** on the wireless networks.
- **The active** attacks are the types of attacks that target the network system and wireless network **to harm the digital resources on the network**. The active attacks are normally done through worms, viruses, Trojan horses and the similar methods.



The other major types of cyberattacks that are unleashed on the wireless network can include the following:

- Distributed attacks
- Phishing attacks
- Password attacks
- Insider attacks
- Hijack attacks
- Close-in attacks

These attacks are normally carried out by exploiting the vulnerabilities and security loopholes in the wireless network and its security mechanisms.



The major vulnerabilities of a wireless security may include the following:

- Reconnaissance vulnerability (Lack of physical security)
- Resource stealing and invasion
- Rogue access points (AP)
- STA and AP plain text transaction
- Denial of service (DoS)
- Default AP configuration
- Rogue insiders
- Protocol vulnerabilities
- Ad-Hoc network mode security problems



Wireless LAN Security Vulnerabilities



HOTSPOT FOR HACKERS

IT'S FREE BUT IT'S **NOT ALL SAFE**



■ Reconnaissance vulnerability...

- The reconnaissance vulnerability is one of the most critical ones in the wireless LAN security system.
- The wireless router of the WLAN network transmits the signals within the rated radius.
- The signals are easily catchable by any hacker that is present in the field of active range of the wireless signals.
- The signals of the wireless network can also be **enhanced and caught through very powerful antennas** used by hackers to access the wireless signals of a remote network.
- The image of a powerful antenna to boost the wireless signals is shown in the figure.





■ Reconnaissance vulnerability

- By using **high power Wi-Fi antennas**, you can boost the strength of signals and **increase the coverage area** of wireless local network.
- Thus, the **reconnaissance vulnerability** of the wireless local area network **increases** with the increased strength of Wi-Fi signals and subsequently the coverage area of the wireless signals.





▪ Resource stealing and invasion

In this type of vulnerabilities, the hackers use the main devices of the wireless network such as, **wireless router** that offers the first layer of the security and the computers devices that have wireless cards.

The routers maintain a routing table and intelligent algorithm for fast routing. **The routing table** is manipulated by using some techniques like IP spoofing and similar; consequently, the device is invaded and befooled to do what the hacker wants to do.

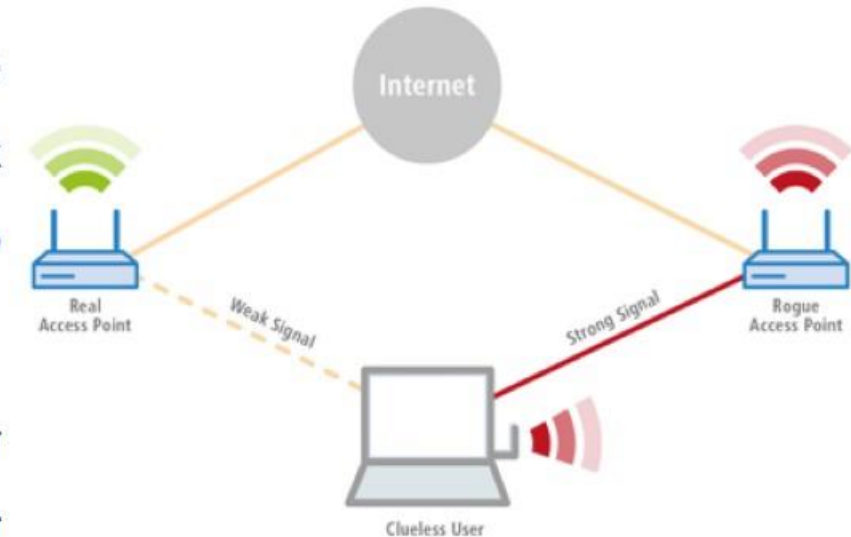
The devices that are connected to the switch through network cables will act as wireless device too due to their wireless enabled cards. This vulnerability is exploited by the hackers very easily to intrude into the security system and steal the useful data that can be used for the lethal cyberattacks on the network of systems.



▪ Rogue access point (AP)...

The **rogue access point** is one of the major vulnerabilities that are exploited by the hackers for **MiTM attacks**. The rogue access points (APs) are those wireless devices that are connected to the network, but have very weak security features or the configuration is done by the physical intruder to access the network in the future.

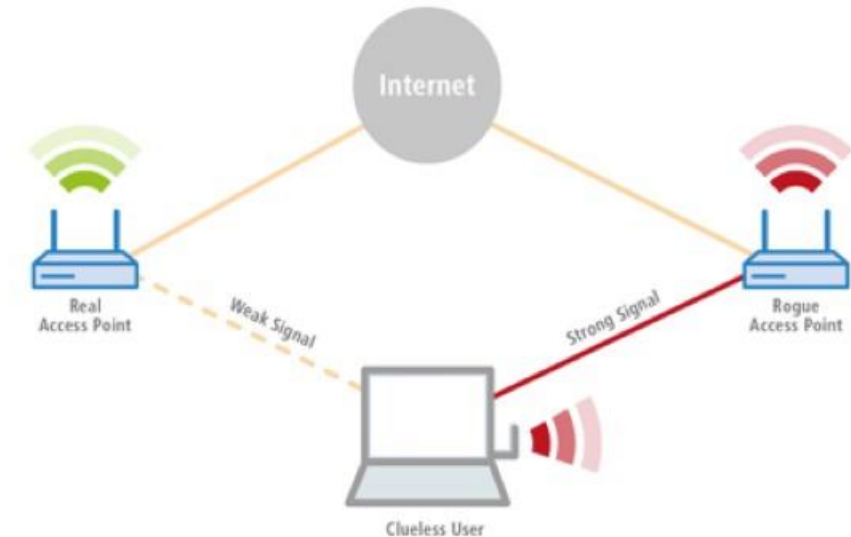
Such APs are normally configured at the edge of the wireless network or away from the security surveillance. Firstly, these APs are then used for passive attacks to steal the information of the network and then the stolen information is used for bigger and more lethal cyberattacks.





▪ Rogue access point (AP)...

- The legitimate users connect to the rogue access point, which is not authorized to work in the network, but it connects the users and routes the traffic through it. The traffic is intercepted and analyzed for the useful data that can help unleash a lethal cyberattack on the network.
- These kinds of **rogue access points** become very nastier in certain cases because the network administrator is fully unaware of the activities of rogue access points that are monitoring the traffic and compromising the network security of the wireless local area network.

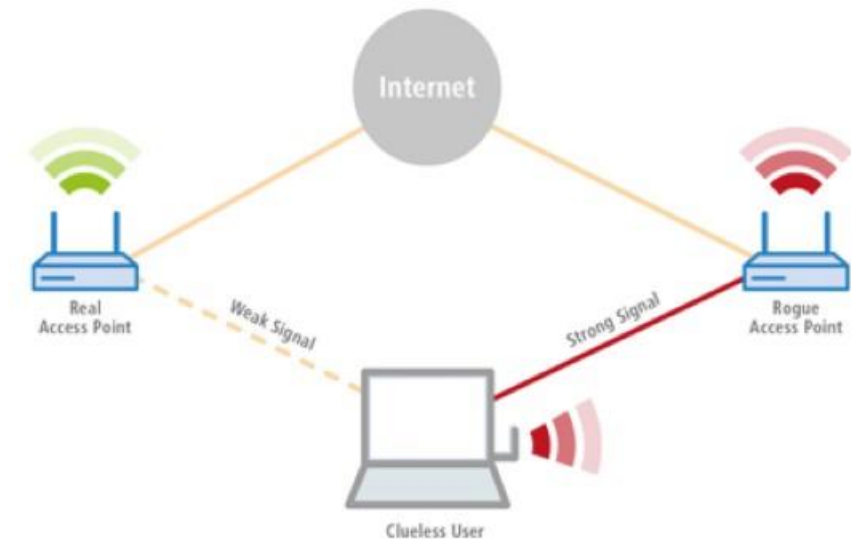




▪ Rogue access point (AP)...

Rogue access points can also be installed on the network by getting physical access to the organization network and placing the access point at some hidden place and connected to the company network switch through a wire.

The physical access is normally achieved by either compromising the physical security or getting help from the accomplice that have access to the physical area of the organization. If a rogue access point installed on the legitimate wireless network the security of the network is at a high risk.





▪ STA and AP plain text transmission...

- The traffic redirection is done by exploiting different vulnerabilities in the network. The main exploits that enable the traffic redirect attack include **phishing and session hijacking through MAC spoofing**.
- It is very important to note that the first communication step between access point (AP) and the legitimate stations commonly referred to as STA takes place in plain text due to encryption/decryption protocols inability at that point.
- The **plain text** information is interrupted by the hackers and thus the information about the **MAC address of access point** as well as legitimate user can be achieved. Once the information about the MAC address is achieved, the hacker can spoof the MAC address and intrude into the network. Once the session is established, the network security can easily be compromised.



▪ Denial of Service (DoS)...

The denial-of-services (DoS) attacks are easier to carryout in wireless networks because of the following factors:

- Easy access to the wireless medium
- Availability of powerful radio devices like wireless cards
- Wireless jammers



In the denial of service attack, one or multiple legitimate users can be prevented from getting access to the network by spoofing the authentication and association sessions.

The client joins the network once the AP authenticated and associated the client or the station (STA). The authentication and association messages can be spoofed as non-legitimate messages and thus, kicking the users out of the services. Thus, the DOS attacks in wireless networks are much easier to exploit than the other networks.



▪ Default AP Configuration...

- The **default configuration** of any access point is a big vulnerability that can put your entire network at a very high-risk of cyberattacks. Normally, the default settings of access points manufactured by any vendor in the world have the known user name and password.
- **For example**, the wireless routers manufactured by the Cisco Systems have the username as Cisco and the password as Cisco. The other manufacturers have the similar types of default standards. The access to the router is free without any password by default.
- And many other security features such as encryption and other standards are by default not configured, so the default configuration can be very dangerous for the security of the wireless network.



▪ Rogue Insiders

The **rogue insiders** are also a big threat for the security of the wireless as well as wired network, but for the wireless network they can be very risky. Hackers can easily exploit the activities of the rogue insiders to compromise the security of the network.

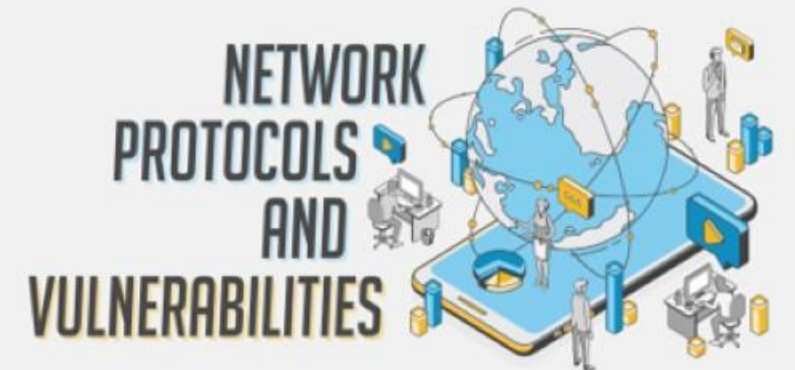
A rogue employee can leak the data of the wireless network as well as he can connect his/her laptop to the network through a wire and provide access to the hackers through wireless card of the computer. The rogue insider can exploit the wireless network very badly.



▪ Protocol Vulnerabilities...

As mentioned in the earlier topics, STA and AP start authentication and association through **plain text** conversation. This is the first vulnerability of the protocol, which can be exploited by the hackers. By exploiting this vulnerability, the hackers can establish a control over the session and then can carry out other malicious activities when they are on the wireless network.

Similarly, the encryption protocols used by the wireless LAN included WEP, WPA, and WPA2. There are certain vulnerabilities in those protocols, which can be exploited by the hackers.





▪ Protocol Vulnerabilities...

For instance, any wireless network using WEP protocol is very insecure. The hackers can break the encryption of WEP within a just one minute's time. It has been marked as expired in the marketplace, but if anybody is using this, he/she is at very high risk.

The **WPA** uses the pre-shared key, which is also vulnerable in the modern security scenario. It uses message integrity checks and temporal key integration protocol (TKIP). The International Consortium for Advancement of Cybersecurity on the Internet (ICASI) has already warned of a few vulnerabilities in even in the **WPA** and **WPA2**. The organization termed the vulnerabilities as Key Reinstallation Attack (KRACK).

By using these vulnerabilities, the hackers can inject some of the specially-crafted packets during the course of authentication handshake. That data packet will force the system to install a key, which is actually controlled by the hackers. Thus, the wireless network using the WPA protocols can also be compromised.



▪ Protocol Vulnerabilities...

The major vulnerabilities of WPA protocol are summarized in the following list:

- It uses encryption RC4, which is vulnerable to DoS attacks
- It uses the MIC value in the EAPoL message in plain text, which is easy for the hackers to attack and break

Similarly, the main vulnerabilities of WPA2 protocol are listed below:

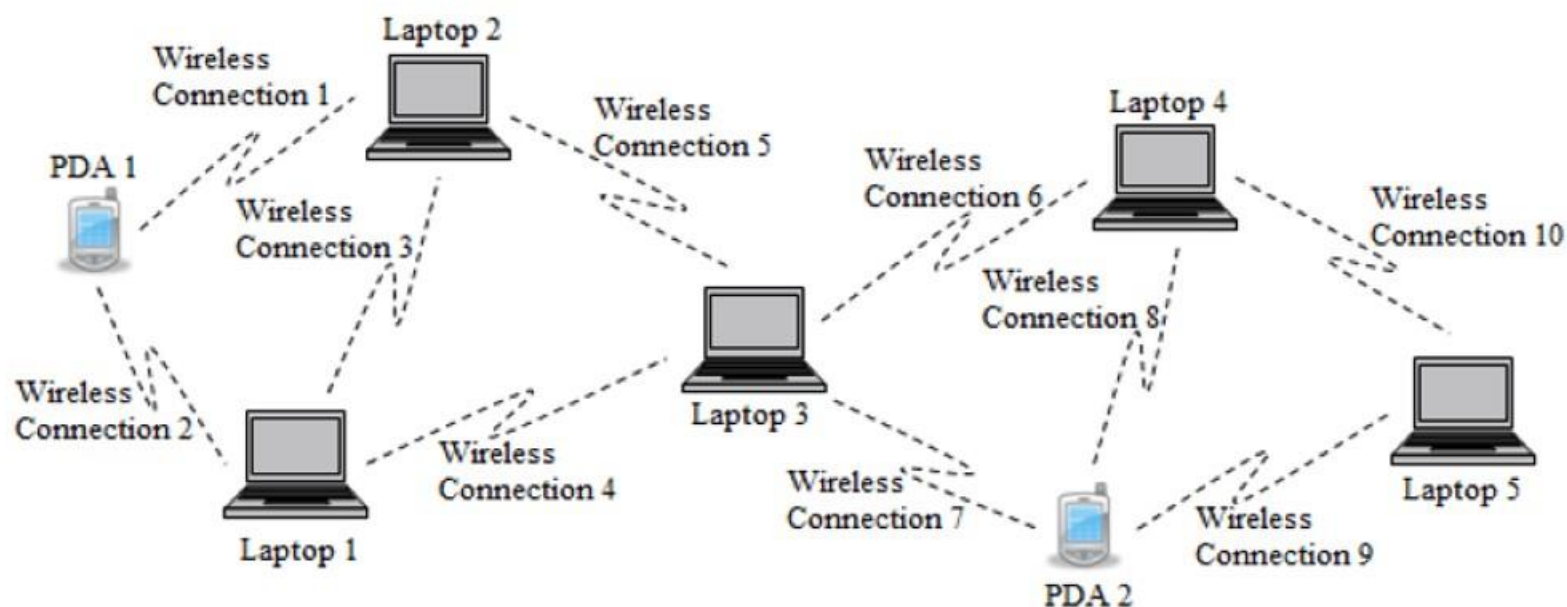
- The 'hole196' is one of the most known vulnerabilities
- CCMP protocol used in WPA2 encryption mechanism is vulnerable to Time-Memory-Trade pre-computation attack

ICASI suggested some guidelines for the manufacturers as well users to avoid the exploitation of those WPA enabled security protocols to avoid any compromise on your wireless local area network security.



▪ Ad-hoc network mode security problems ...

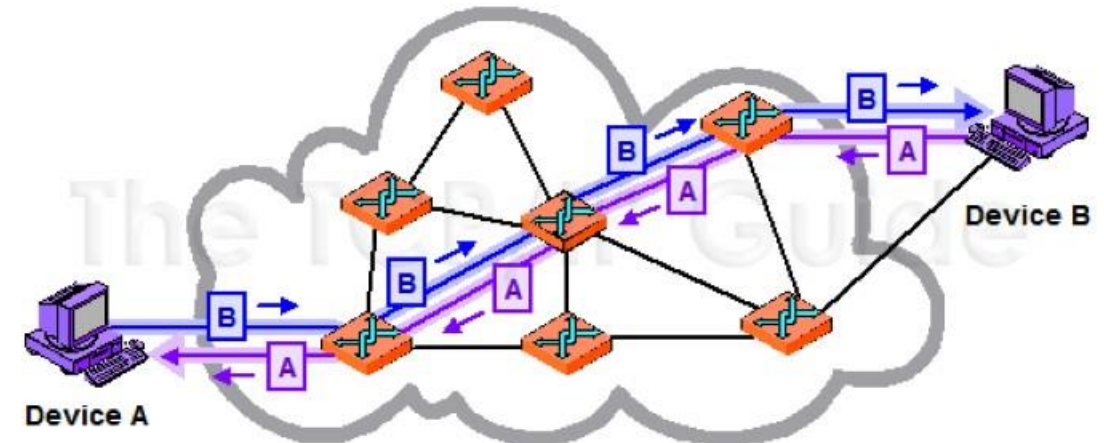
The use of ad-hoc networking is supported by many operating systems including the Windows operating system. By using ad-hoc network, every host in the network can communicate with the other network based on agreed SSID. **This type of wireless network is very vulnerable in terms of security because there is no firewall behind this network.**





The wireless wide area network is the wireless network spread over large area of operation. The main examples of wireless wide area networks include the 2G, 3G, 4G, and 5G networks. All mobile broadband networks are the examples of wide area networks. The wireless wide area networks can be classified into two sections as listed below:

- Circuit switch data network
- Packet switch data network



The security of the wide area network is implemented by the internet service providers commonly known as the ISPs. The security of those wireless WAN networks is mostly implemented at the **protocol, system backbone, and base-stations of the network.**



The **main protocols** used in the **circuit switched data** networks for the authentication of the users include, **PAP, CHAP, and SPAP**. These protocols have their own pros and cons in terms of their security and other features.

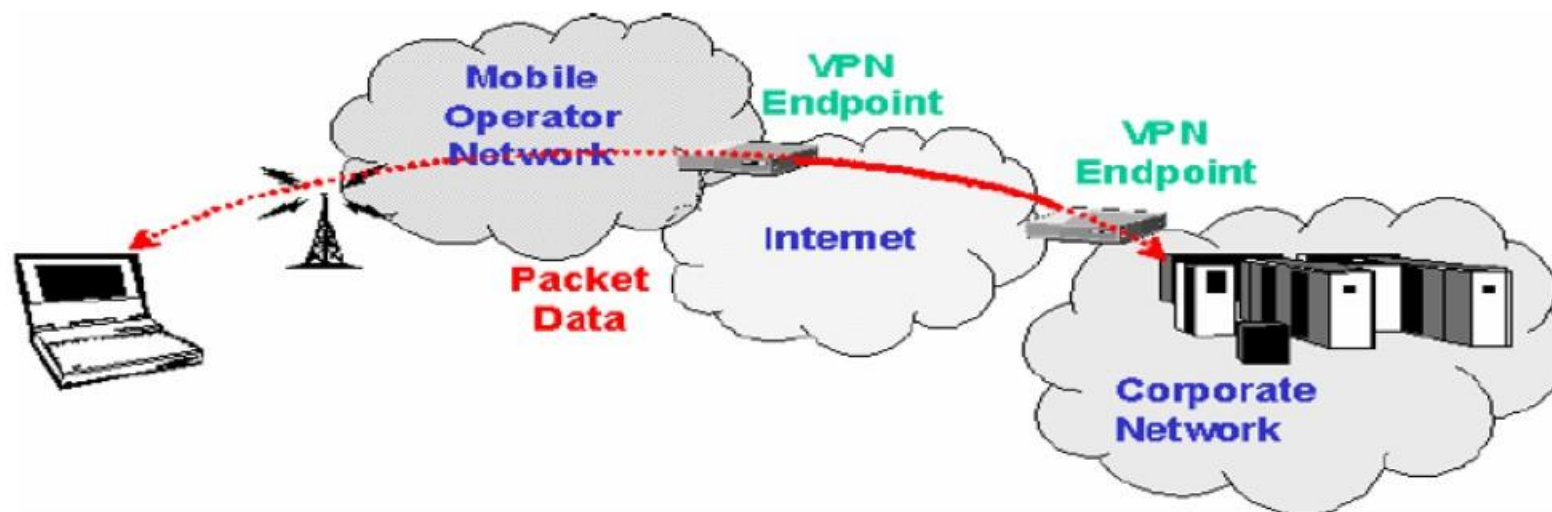
There are certain wireless WAN vulnerabilities that are given below:

- Password Authentication Protocol (PAP) is normally used for authentication, which uses the plaintext messages without any encryption for getting the username and passwords for authentication
- Circuit switched network uses public network prone to cyber threats

The other form of Wireless WAN is based on the **packet switching**. This network uses the packet routing that takes place from multiple routers and always from the different paths.



The data transfer **is also encrypted**. The schematic diagram of a packet switched wide area network powered by wireless technology is shown below:



So, the **security of this network** is much stronger than the previous types of wide area network. This type of network uses **the point to point VPN connection** so, the security of the data much higher than the other forms.



Internet of things (IoT) is a type of networking technology, which is in the market for quite a few years now. It is a network of IP enabled devices all connected in a networked environment and controlled through a centralized control unit. The examples of IP enabled devices include the all main appliances and machines that we use in our day to day life. For example, printer, door-lock, fridge, AC, heater, water tank, cooker, micro-wave oven and many others.

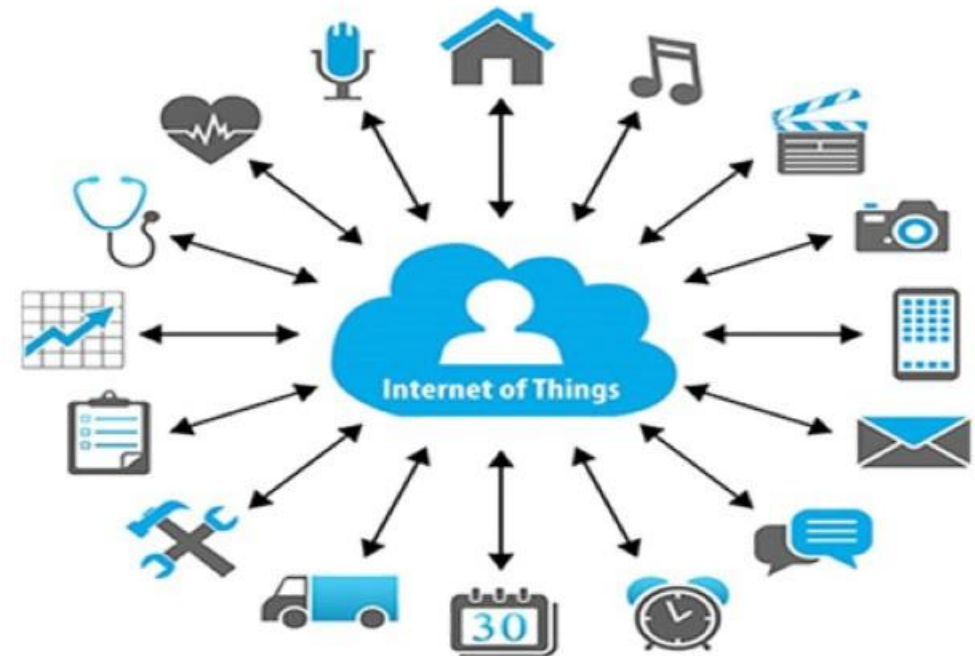
According to the Statista predictions, the total number of connected devices worldwide will cross the 75.44 billion by 2025. The present number of IoT connected devices worldwide is about 26.66 billion in 2019.





The major driver of this technology is the **centralized wireless network** that connects the devices altogether at office, home, shopping mall, even in the industry. **The centralized unit** and the other nodes in an office or home connect to the central control unit through wireless networks that include the following wireless networks:

- Low Power Wide Area Network (LPWANs)
- Bluetooth Low Energy (BLE) and Bluetooth networks
- Cellular technologies like 5G, 4G, 3G and others
- Radio Frequency Identity (RFID)
- Wi-Fi network
- ZigBee network
- Z-wave





The main challenges related to the security of IoT network include the following:

- Securing the wireless enabled connected devices
- Updating the firmware and software of the devices
- Securing communication between the nodes
- Detecting vulnerabilities at different levels of the network
- Securing the authentication and authorization process of connected devices
- Security of mobile and web applications used in managing the network
- Wireless connectivity security
- Ensuring the data integrity and privacy
- Security of cloud applications
- Maintaining stability of a complex network



Wireless networks are more prone to risks as compared to the wired networks owing to their signals going out of the boundaries of your home and organization. A hacker can easily catch the wireless signals and use the sophisticated techniques to intrude into your wireless network.

You need to consider the level of security that you require for your data and other resources on your network. If you are running a business and have business information on your network, you should consider developing a proper security policy so that you can manage your security at higher level.

If you want to secure your home network with less important data on the network, you can take general guidelines and security measures that can help you secure your home network.



Let's have a look at the major security measures that can help you secure your home or office wireless networks.



- Modify Default Configuration
- Wireless Router Location
- Update Router Software
- Stronger Encryption Algorithms
- MAC Address Filtering



■ Modify default configuration ...

The default settings of your wireless router or other nodes of your wireless network are common and known to everybody with a little technical knowledge. You should modify all major default configurations to new ones. The configuration interface of most commonly used Linksys router is given in Fig.:

LINKSYS
A Division of Cisco Systems, Inc. Firmware Version: v3.00.1

Setup Wireless-G Broadband Router **WRT54G**

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name:

Host Name:

Domain Name:

MTU: Auto

Size:

Network Setup

Router IP

Local IP Address:

Subnet Mask: 255.255.255.0

DHCP Server: ☒ Enable ☐ Disable

Starting IP Address:

Maximum Number of DHCP Users:

Client Lease Time: minutes (0 means one day)

Automatic Configuration - DHCP: This setting is most commonly used by Cable operators.

Host Name: Enter the host name provided by your ISP.

Domain Name: Enter the domain name provided by your ISP.

More...

Local IP Address: This is the address of the router.

Subnet Mask: This is the subnet mask of the router.

DHCP Server: Allows the router to manage your IP addresses.

Starting IP Address: The address you would like to start with.

Maximum number of DHCP



▪ Modify default configuration

You should use unique names, numbers and passwords that are strong and difficult for the other people to guess. **You should also add new data for the following parameters of your wireless router.**

- Service set identifier (SSID)
- Administrator username and passwords
- Remote access feature
- Enable stealth mode (Hide)
- Network partitions (Vlan)
- WPA2 password
- Enable stronger encryption



▪ Wireless router location

The **location** of the router either in office or home is very important. The location of the router affects the wireless network performance as well as the security of the network. The Wi-Fi router should be placed at the centralized location where the signals of good strength reach to all legitimate users, but outsiders don't get signals strong enough to connect. Thus, you will lay strong foundation for the network security by placing the router at very suitable location in the office or home.





▪ Update router software

All manufacturers of Wi-Fi routers and other networking devices always release new software patches and software updates. Those updates are developed to remove any bug or vulnerability in the software. In a wireless network, you should always make sure that your routers as well as other networking devices are updated regularly.

It is highly recommended to check for any new updates in the administration interface of the router and download to install the new patches or versions of the software. This will prevent your wireless network from any cyber threat. Many routers update automatically, if you set the configuration to automatic update. This will prevent from regular checking for the software updates.





▪ Stronger encryption algorithm

Encryption is the method to scramble the data and communication messages into a fixed code so that the hackers are not able to decode those messages. Wireless network routers support different types of encryption algorithms, which make them secure according to their features and capabilities. Among such encryption algorithms **WEP**, **WPA**, **WPA2**, and **WPA3** are a few important algorithms that are supported by the modern wireless routers.

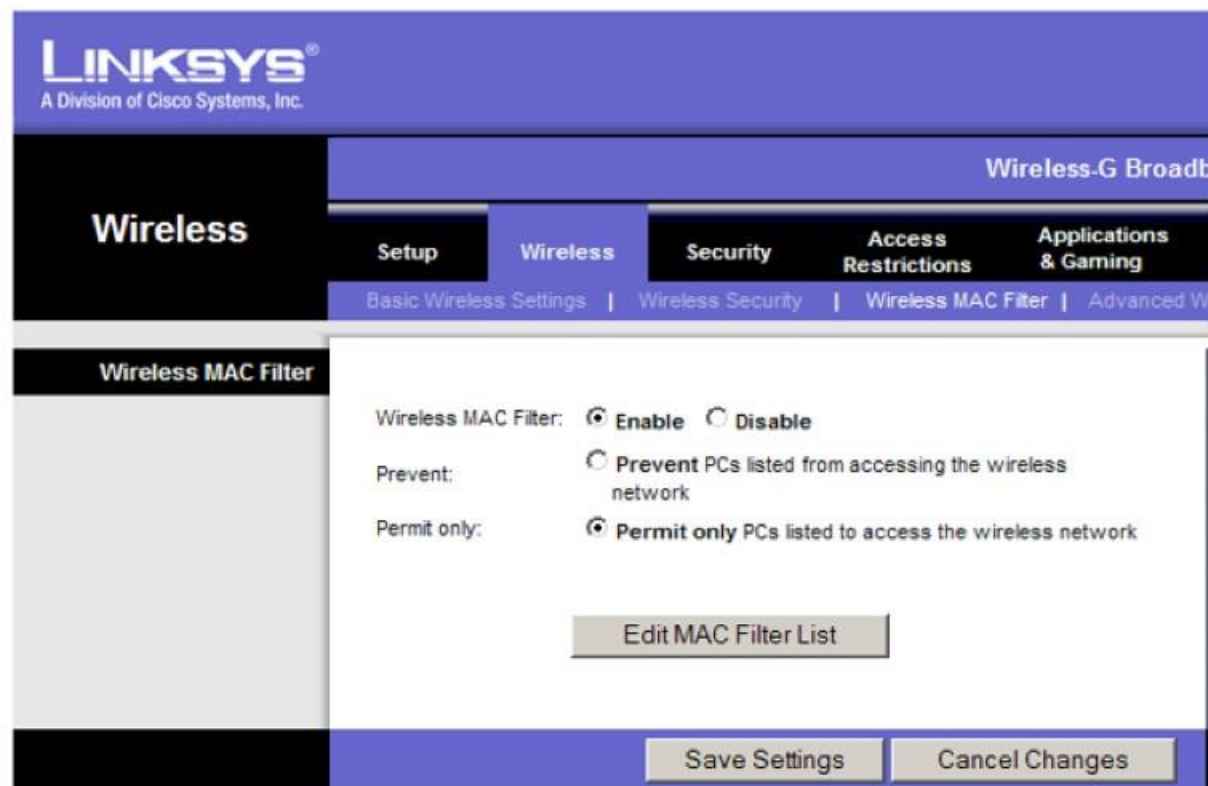
To make your wireless network security stronger use the latest encryption method like **WPA2** or **WPA3** so that your network remains secure from any attack on data integrity.





▪ MAC address filtering ...

MAC address filtering is process in which Wi-Fi router checks and verifies the MAC address of the device that send connection request whether to allow it to connect or not. This feature normally done manually to add the MACs of the devices that you want to allow connecting to the wireless network. By doing this, your Wi-Fi router will not allow any device to connect other than the devices whose MAC addresses are already added in the allowed list.





Wireless network is more vulnerable as compared to the other wired networks; so, it is highly recommended to follow the standard and industry guidelines while using the wireless networks either at home or at office.

Many security experts, standards' organizations and regulators agree upon the following main tips for using the wireless network securely:

- Always change the default settings of your router and other networking devices
- Use very strong admin and pass-code passwords that are longer and include capital letters, lowercase letters, numbers, and symbols
- Always keep your wireless router in stealth mode so that your router does not broadcast the SSID on the air interface



- The SSID should be longer and more robust to maintain high security
- Turn on strong encryption mechanism like WPA2 or more advanced algorithms, such as Advanced Encryption Standard (AES)
- Disable the Wi-Fi protected setup (WPS) feature
- Always keep the Universal Plug N Play (uPnP) feature disabled
- Always configure manual MAC address binding with internet connection on your router so that no other device can connect to your network
- Disable the auto-connection feature on all your network and computer devices so that they don't connect to the routers of the neighbors and insecure hotspots
- Always search for the rogue routers (access points) on your network coverage area. If you find rogue AP, remove it and take the security steps to avoid such things in the future



- Always use security firewalls on your network so that it can block any external threat
- Use static IPs for the devices that you use. This is a bit cumbersome to configure static IPs manually, but offer great security
- Turn off the network elements, if not in use for longer periods
- Change the default IP address of your router and configure other IP address
- Never enable the remote administrator access to your router, this will increase the risk of cyberattacks on your router
- The software on your router and other nodes should be always up to date. It is good idea to enable auto-update option on your network devices so that any new patch or software release is automatically installed



- Always configure a separate network with limited authority for the guest users to avoid any intentional and unintentional malicious activity on the network
- If possible, use a VPN connection for secure, private and anonymous browsing
- Always use the Ethernet cable to access the control panel of the wireless router and try to avoid the use of wireless connectivity to access the control panel
- Locate your wireless router at the central location of your place so that the signals are contained within the boundaries of your place
- Turn off the wireless router, if not in use
- All of the above guidelines should be implemented on-time without any delay. If you put today's task on tomorrow in wireless network environment, your network security is at risk



SAMPLE QUESTIONS AND ANSWERS FOR WHAT WE HAVE LEARNED IN CHAPTER 9

See Reference Book Page 217-218



Thank You