



NETWORK SECURITY ESSENTIALS

BCA – IV

Credits – 4

Evaluations – 5

The course is designed to build an understanding of various network security components, protocols and creating the awareness about the issues due to security.

Pre-requisites: An understanding of Basic Computer Networking and security

UNIT 6

- Wireless Communications and 802.11 WLAN Standards
- WEP, WPA
- IEEE 802.11i/WPA2
- Bluetooth Security



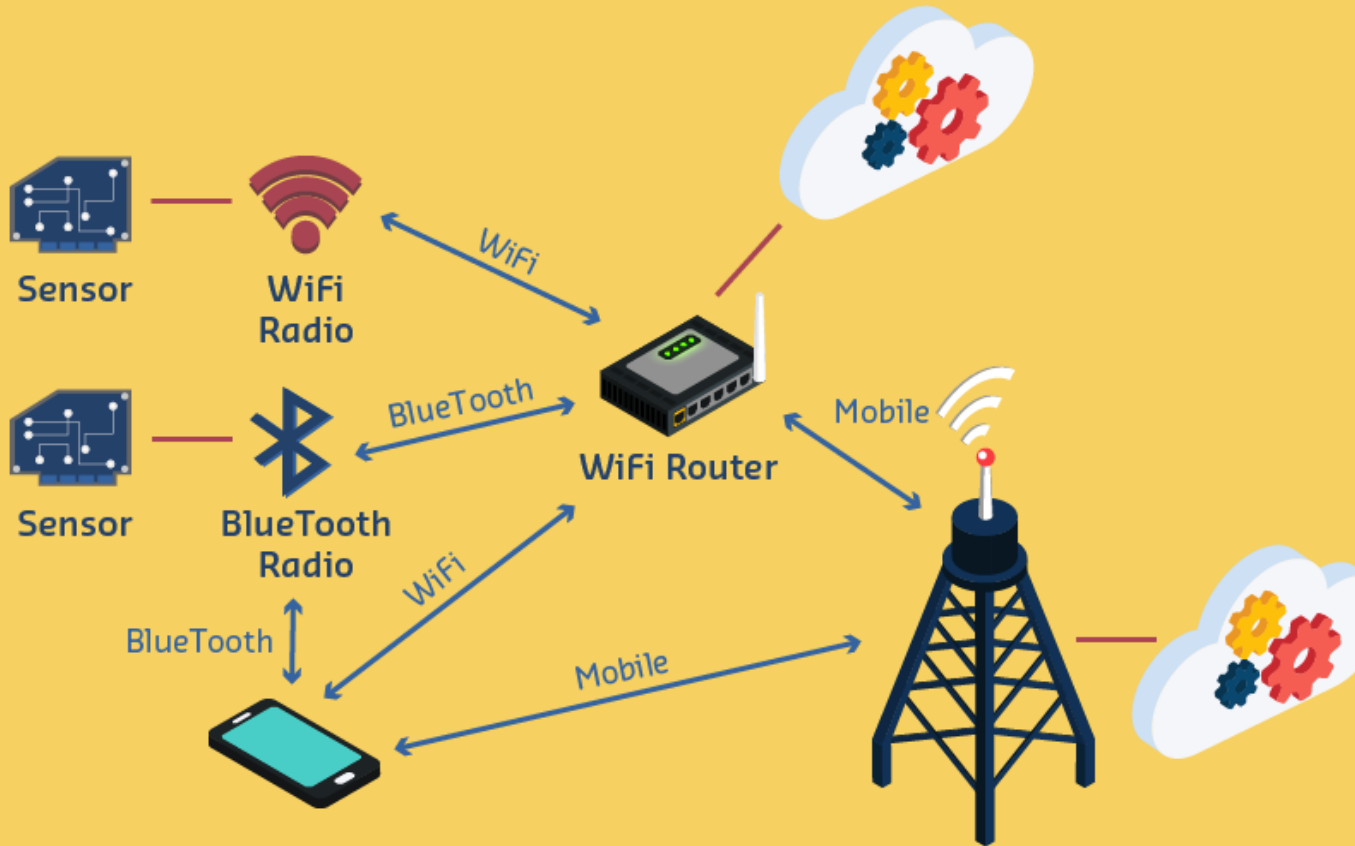
WIRELESS COMMUNICATION

Wireless Communication is the fastest growing and most vibrant technological areas in the communication field. Wireless Communication is a method of transmitting information from one point to other, without using any connection like wires, cables or any physical medium.

Generally, in a communication system, information is transmitted from transmitter to receiver that are placed over a limited distance. With the help of Wireless Communication, the transmitter and receiver can be placed anywhere between few meters (like a T.V. Remote Control) to few thousand kilometers (Satellite Communication).

Some of the commonly used Wireless Communication Systems in our day – to – day life are: Mobile Phones, GPS Receivers, Remote Controls, Bluetooth Audio and Wi-Fi etc.

WHY WIRELESS COMMUNICATION?



When wired communication can do most of the tasks that a wireless communication can, why do we need Wireless Communication? The primary and important benefit of wireless communication is mobility.

Apart from mobility, wireless communication also offers flexibility and ease of use, which makes it increasingly popular day – by – day. Wireless Communication like mobile telephony can be made anywhere and anytime with a considerably high throughput performance.

Another important point is infrastructure. The setup and installation of infrastructure for wired communication systems is an expensive and time consuming job. The infrastructure for wireless communication can be installed easily and low cost.

In emergency situations and remote locations, where the setup of wired communication is difficult, wireless communication is a viable option.

ADVANTAGES OF WIRELESS COMMUNICATION

Cost

The cost of installing wires, cables and other infrastructure is eliminated in wireless communication and hence lowering the overall cost of the system compared to wired communication system. Installing wired network in building, digging up the Earth to lay the cables and running those wires across the streets is extremely difficult, costly and time consuming job.

Mobility

As mentioned earlier, mobility is the main advantage of wireless communication system. It offers the freedom to move around while still connected to network.

Ease of Installation

The setup and installation of wireless communication network's equipment and infrastructure is very easy as we need not worry about the hassle of cables. Also, the time required to setup a wireless system like a Wi-Fi network for example, is very less when compared to setting up a full cabled network.

Reliability

Since there are no cables and wires involved in wireless communication, there is no chance of communication failure due to damage of these cables, which may be caused by environmental conditions, cable splice and natural diminution of metallic conductors.

Disaster Recovery

In case of accidents due to fire, floods or other disasters, the loss of communication infrastructure in wireless communication system can be minimal.

DISADVANTAGES OF WIRELESS COMMUNICATION

Interference

Wireless Communication systems use open space as the medium for transmitting signals. As a result, there is a huge chance that radio signals from one wireless communication system or network might interfere with other signals.

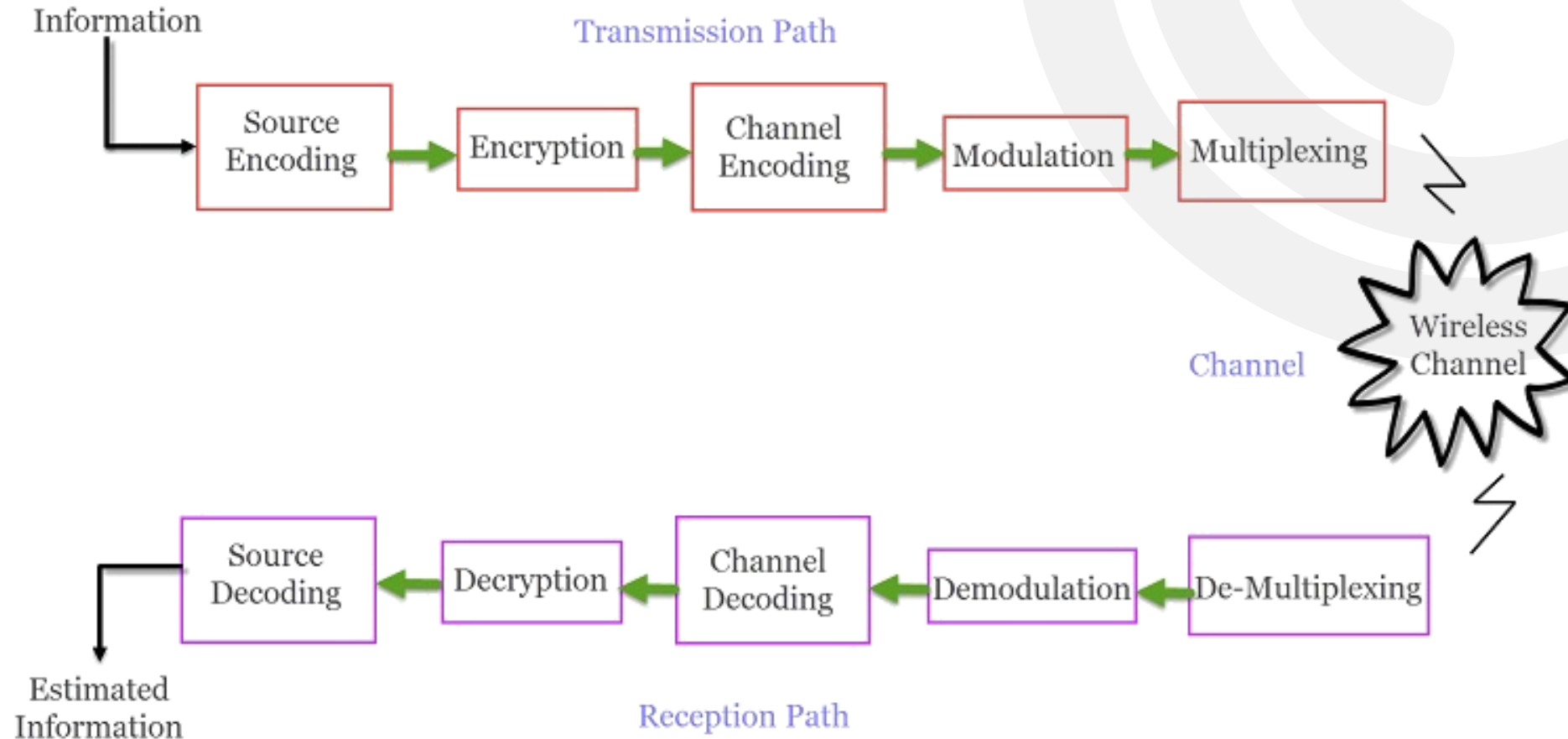
Security

One of the main concerns of wireless communication is Security of the data. Since the signals are transmitted in open space, it is possible that an intruder can intercept the signals and copy sensitive information.

Health Concerns

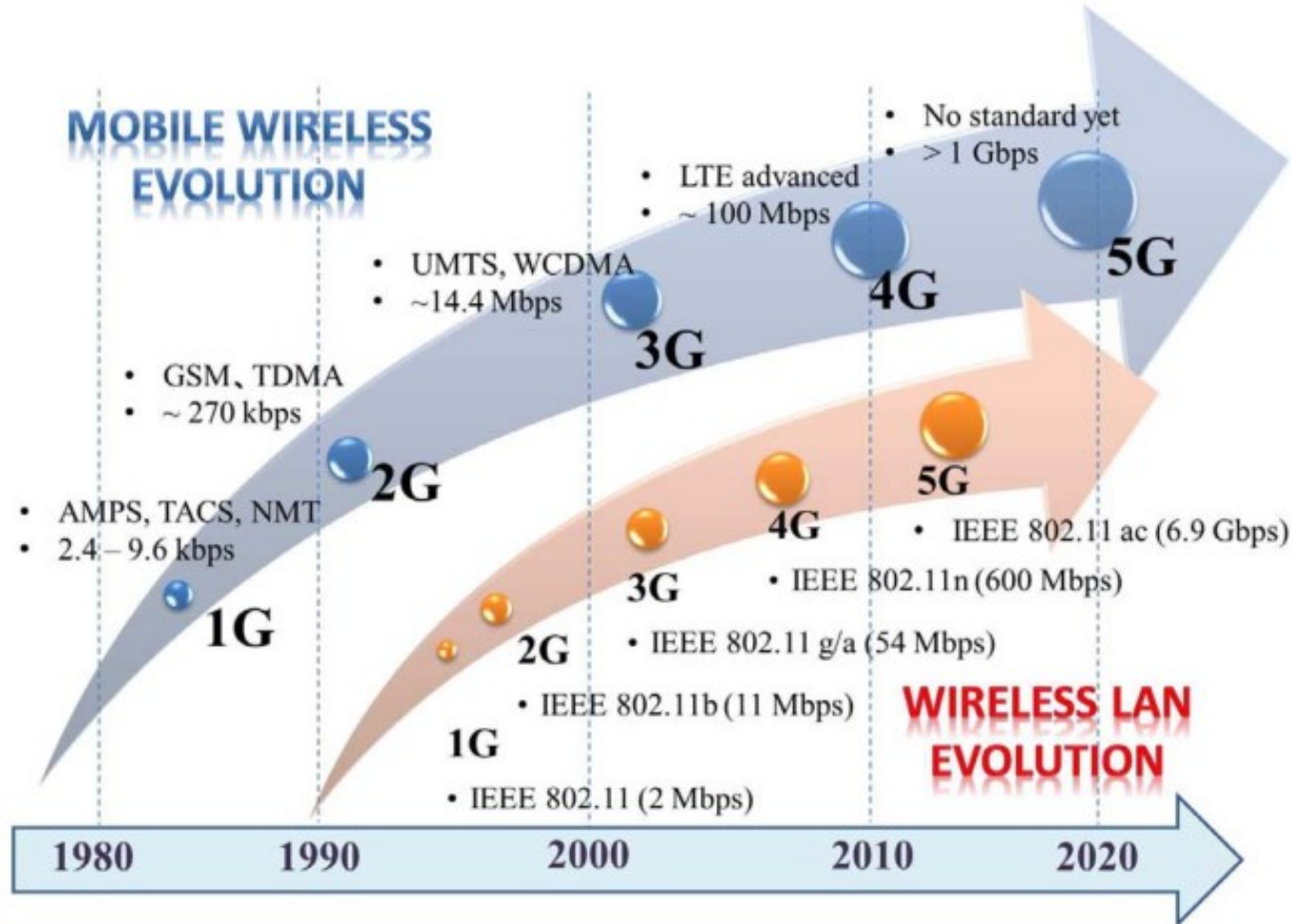
Continuous exposure to any type of radiation can be hazardous. Even though the levels of RF energy that can cause the damage are not accurately established, it is advised to avoid RF radiation to the maximum.

BASIC ELEMENTS OF A WIRELESS COMMUNICATION SYSTEM



A typical Wireless Communication System can be divided into three elements: the Transmitter, the Channel and the Receiver.

TYPES OF WIRELESS COMMUNICATION SYSTEMS



Some of the important Wireless Communication Systems available today are:

- Television and Radio Broadcasting
- Satellite Communication
- Radar
- Mobile Telephone System (Cellular Communication)
- Global Positioning System (GPS)
- Infrared Communication
- WLAN (Wi-Fi)
- Bluetooth
- Zigbee
- Paging
- Cordless Phones
- Radio Frequency Identification (RFID)

CONCEPTUAL LAYERS IN A WIRELESS NETWORK

Physical layer---involves the actual signal transmission and reception over the propagation channel.

Datalink Link layer---deals with signal at the output of the base station receiver, performs radio resource management, power control, rate allocation, call admission, error control etc.

Networks layer: a protocol stack that includes handoff management, location management, traffic management and traffic control.

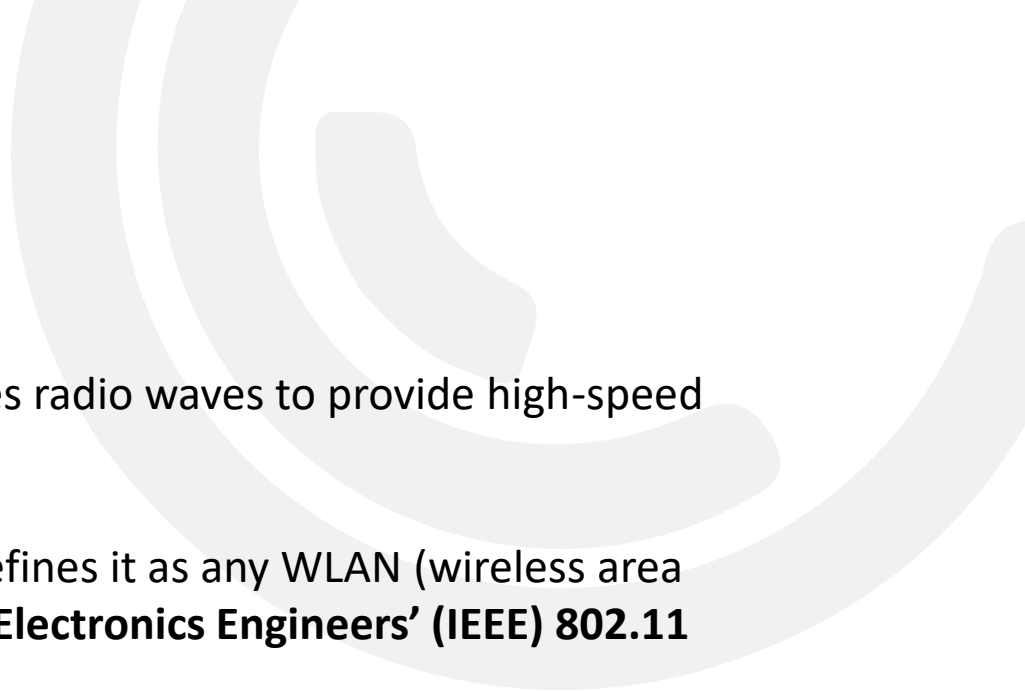
Application layer: communicating, distributed processes running in end systems (hosts), e.g., e-mail, Web, P2P file sharing, instant messaging

WI-FI



Wi-Fi is a low power wireless communication, that is used by various electronic devices like smartphones, laptops, etc. In this setup, a router works as a communication hub wirelessly. These networks allow users to connect only within close proximity to a router. WiFi is very common in networking applications which affords portability wirelessly. These networks need to be protected with passwords for the purpose of security, otherwise, it will be accessed by others.

The WiFi router is the medium which receives the internet connection via a wide area network (WAN) port. WiFi stands for Wireless Fidelity and is the same thing as saying WLAN which stands for "Wireless Local Area Network."



Wi-Fi is trademarked name for popular wireless technology that uses radio waves to provide high-speed Internet and network connections.

The governing body that owns the term Wi-Fi, the Wi-Fi Alliance, defines it as any WLAN (wireless area network) products that are based on the **Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.**

The way Wi-Fi works is through the use of radio signals like in phones. The wireless adapter card that is found inside of computers then uses the data that is being sent to change it into a radio signal to then be transmitted by the antenna. A router then receives these signals and decodes them in order to send the information contained within to the Internet via a Local Area Network or a wired Ethernet connection like a cable network connection.

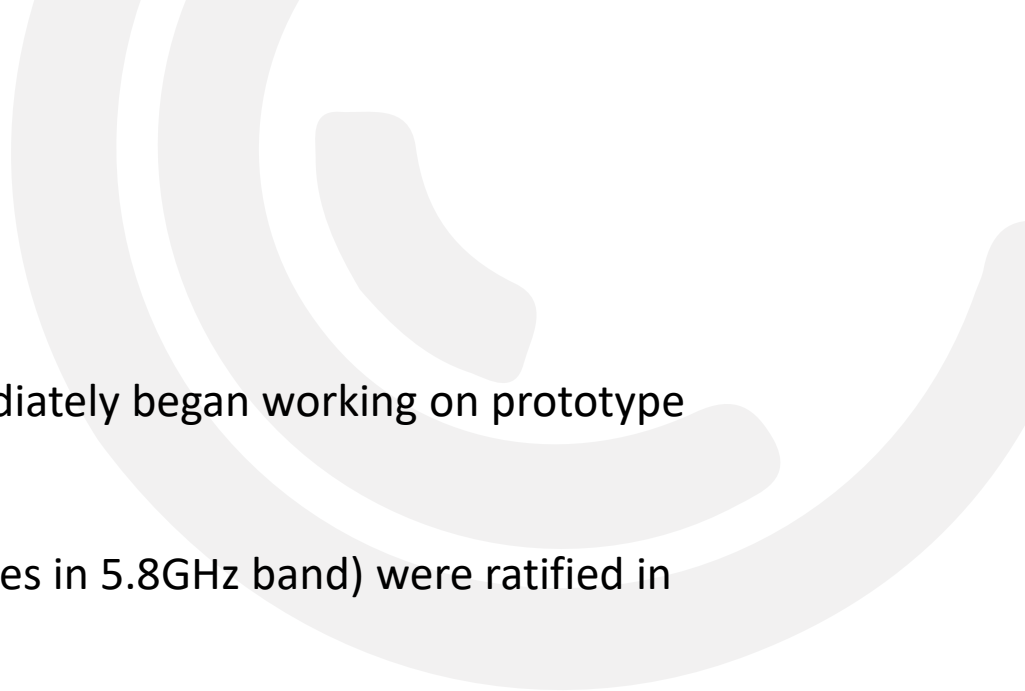
In 1985 the Federal Communications Commission (FCC) allowed the opening of several bands of the wireless spectrum. Allowing those bands to be used without government license.

The bands were taken from the scientific, medical, and industrial bands of the wireless spectrum. The FCC made these bands available for communication purposes.

Using spread spectrum technology, which spreads a radio signal over wide range of frequencies they were able to steer around interference from other equipment. When Ethernet became popular vendors came to the realization that a wireless standard was best.

In 1988, the NCR Corporation wanted to use the unlicensed spectrum to hook up wireless cash register, they looked into getting a standard started. Victor Hayes and Bruce Tuch were hired and they went to the IEEE and created the committee known as 802.3.

Vendors took a while to agree on an acceptable standard due to the fragmented market. In 1997 the committee agreed on a basic specification that allowed for a data-transfer rate of two megabits per second. Two technologies known as frequency hopping, and direct-sequence transmission allowed for this data-transfer rate.



The new standard was finally published in 1997, and engineers immediately began working on prototype equipment that was compliant.

Two variants 802.11b (operates in 2.4GHz band), and 802.11a (operates in 5.8GHz band) were ratified in December 1999 and January 2000 respectively.

In August 1999 the Wireless Ethernet Compatibility Alliance (WECA) was created with the intention to assure compatibility between products from various vendors. A consumer friendly name was need for this new technology and the term “Wi-Fi” came to be.

Apple was the first to supply their computers with Wi-Fi slots on all their laptops, thus sparking the mainstream penetration of Wi-Fi.

WIFI FREQUENCIES

A wireless network will transmit at a frequency level of 2.4 GHz or 5GHz to adapt to the amount of data that is being sent by the user. The 802.11 networking standards will somewhat vary depending mostly on the user's needs.

The **802.11a** will transmit data at a frequency level of 5GHz. The Orthogonal Frequency-Division Multiplexing (OFDM) used enhances reception by dividing the radio signals into smaller signals before reaching the router. You can transmit a maximum of 54 megabits of data per second.

The **802.11b** will transmit data at a frequency level of 2.4GHz, which is a relatively slow speed. You can transmit a maximum of 11 megabits of data per second.

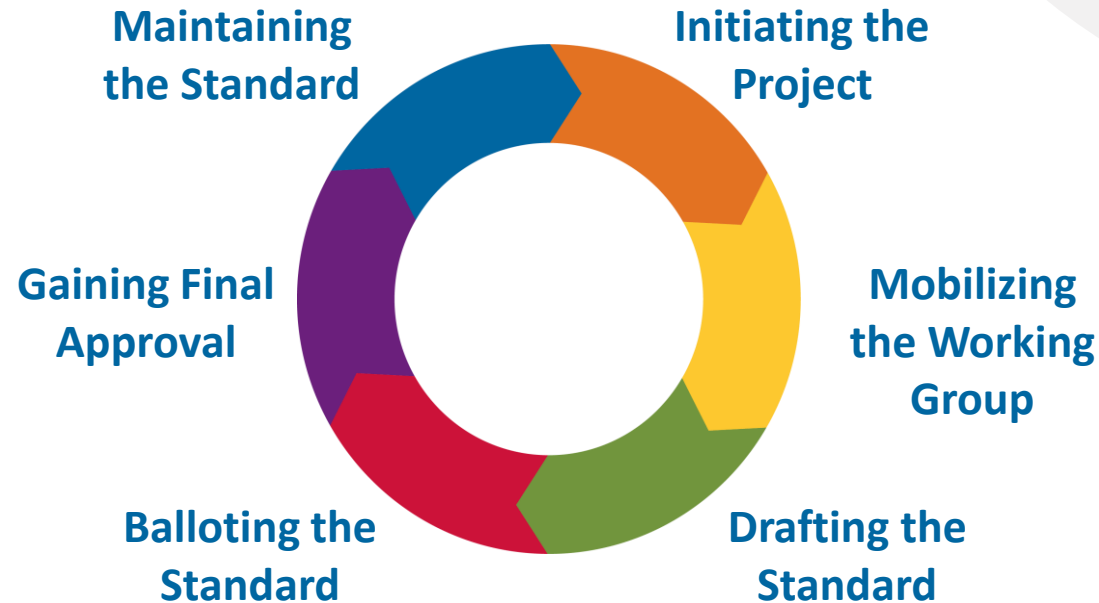
The **802.11g** will transmit data at 2.4GHz but can transmit a maximum of 54 megabits of data per second as it also uses an OFDM coding.

The more advanced **802.11n** can transmit a maximum of 140 megabits of data per second and uses a frequency level of 5GHz.

The term **hotspot** is used to define an area where WiFi access is available. It can either be through a closed wireless network at home or in public places such as restaurants or airports.

IEEE 802.11 OVERVIEW

IEEE Standards drive the functionality, capability, and interoperability of a range of products and services that affect the way people live, work, and communicate.



The 802.11 Working Group was established in 1990.

The IEEE 802.11 Working Group is one of the most active WGs in 802

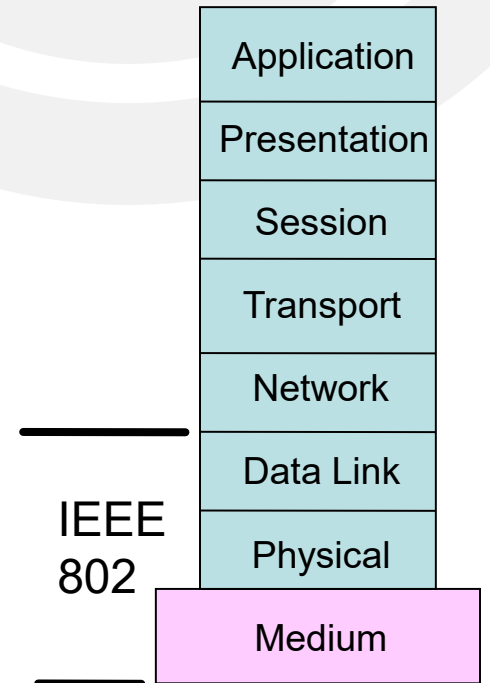
- Focus on **link and physical layers** of the network stack
- Leverage IETF protocols for upper layers

The first standard was published in 1997 (2.4GHz) supporting 1 and 2 Mbps.

Subsequent amendments and revisions have increased radio performance and throughput by orders of magnitude.

The 802.11b 11Mbps standard was the first to achieve commercial success, with the announcement by Steve Jobs at MACWorld in 2001 that the MacBook would include 802.11 radios, along with the Apple Airport. PC vendors followed suit. Describe highlights of each revision.

OSI Reference Model



WEP/WPA

WEP was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks, however there are a lot of well-known security issues in WEP, which is also easy to break and hard to configure.

Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

For the time the 802.11i wireless security standard was in development, WPA was used as a temporary security enhancement for WEP. One year before WEP was officially abandoned, WPA was formally adopted. WPA Enterprise uses an authentication server for keys and certificates generation.

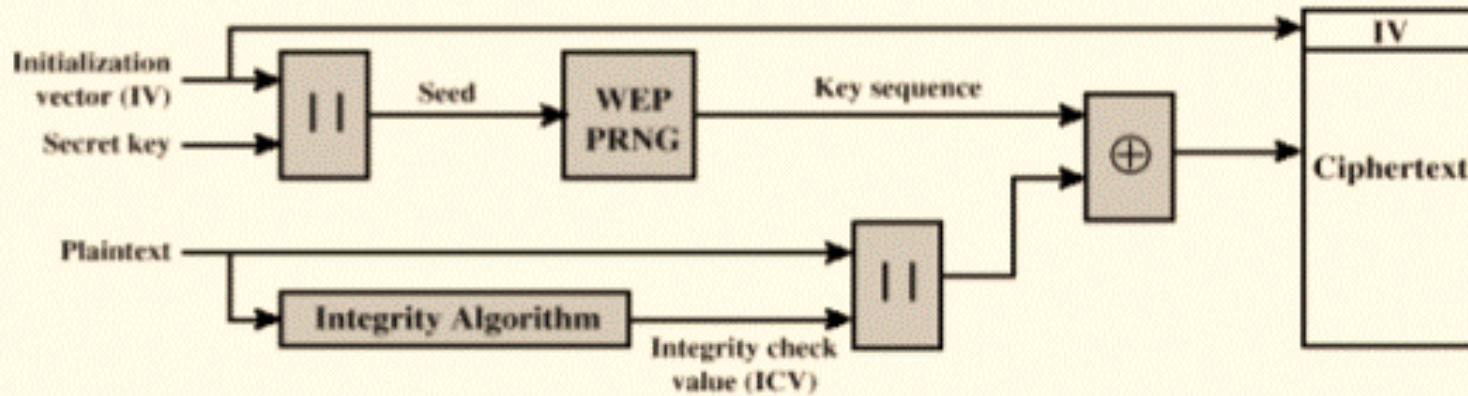
WPA was a significant enhancement over WEP, but as the core components were made so they could be rolled out through firmware upgrades on WEP-enabled devices, they still relied onto exploited elements.

WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion. The attacks that posed the most threat to the protocol were however not the direct ones, but those that were made on Wi-Fi Protected Setup (WPS) - auxiliary system developed to simplify the linking of devices to modern access points.

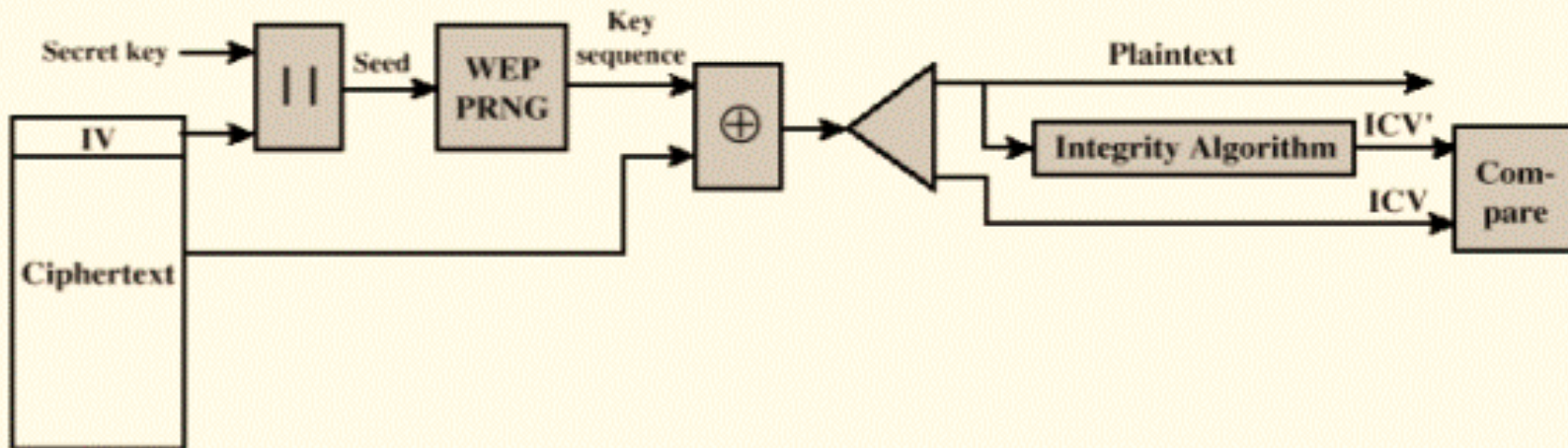
WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network. As wireless networks transmit data over radio waves, eavesdropping on wireless data transmissions is relatively easier than in wired networks connected by cables. WEP aims to provide the same level of security and confidentiality in wireless networks as in wired counterparts.

WEP Encryption/Decryption



(a) Encryption



(b) decryption

SECURITY ISSUES WITH WEP

WEP uses the stream cipher RC4 for confidentiality. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5,000 packets.

Furthermore,

- the use of WEP was optional, resulting in many installations never even activating it, and
- by default, WEP relies on a single shared key among users, which leads to practical problems in handling compromises, which often leads to ignoring compromises.

WPA – WIFI PROTECTED ACCESS

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP).

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

In January 2018, Wi-Fi Alliance announced the release of WPA3 with several security improvements over WPA2.

WPA also referred to as the draft IEEE 802.11i standard became available in 2003. The Wi-Fi Alliance made it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 which is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

WEP uses the RC4 algorithm for encryption, which is supported in hardware. Most wireless equipment only supported RC4 and not a more advanced encryption algorithm like AES. We know that WEP is insecure, so to make sure that the older hardware could still use a secure encryption method, IEEE developed the Temporal Key Integrity Protocol (TKIP).

WPA uses **Temporal Key Integrity Protocol (TKIP)**, which recycled some items from WEP; it still uses the RC4 algorithm. Some things are improved; for example, TKIP uses 256-bit keys instead of the 64 and 128-bit keys in WEP.

Unfortunately, WPA was doomed from the start. It was based on parts of the 802.11i standard, which was still a draft. It was good enough to replace WEP and use existing hardware, but in the long run, something else was needed.

TKIP adds the following security features:

MIC: We have an extra message integrity check called Michael, which adds a hash value to each frame. We use this so we can detect if someone made changes to the frame.

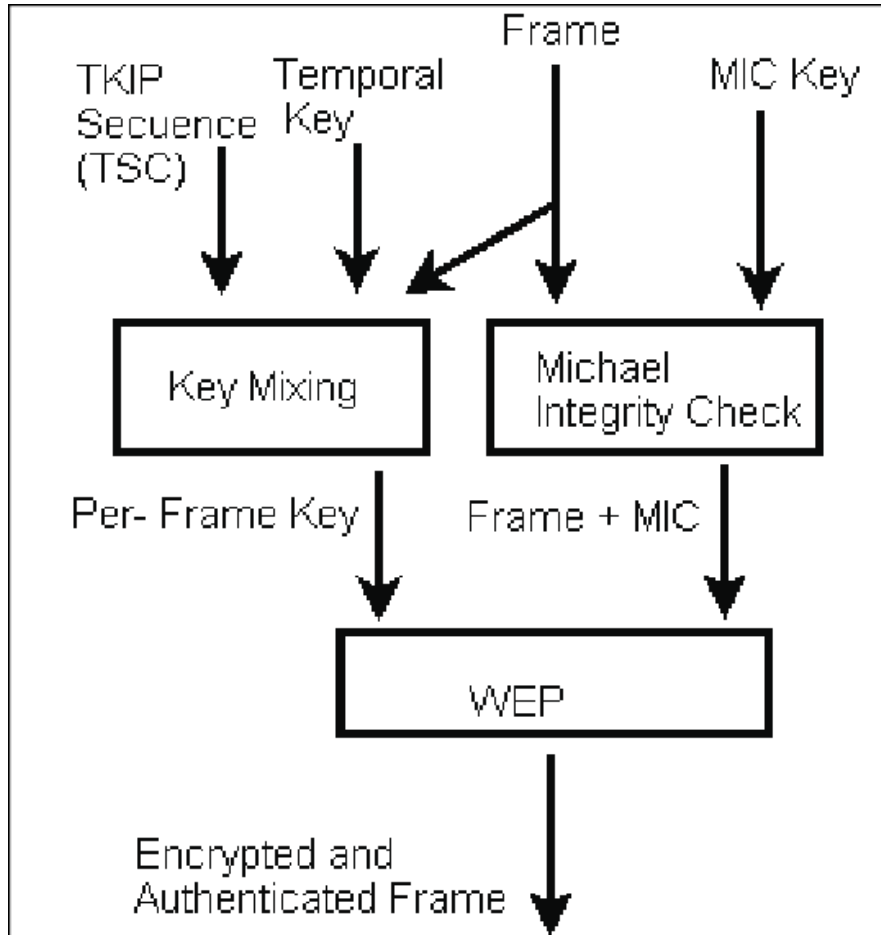
TKIP sequence counter: This counter provides a record of frames sent by each MAC address. We use this so an attacker can't perform a replay attack by retransmitting frames.

Key mixing algorithm: This algorithm calculates a unique 128-bit WEP key for each frame.

A longer initialization vector (IV): The IV size is 48 bits, versus 24 bits for WEP. This makes it much harder to brute force calculate all WEP keys.

Timestamp: We add a timestamp to the MIC to prevent replay attacks. A replay attack attempts to retransmit a frame that was previously sent.

Sender MAC address: The MIC includes the sender's MAC address. This is used to prove who the actual sender of the frame is.



TKIP was a temporary solution, while IEEE worked on the 802.11i standard. Nowadays, TKIP also has vulnerabilities, and you shouldn't use it anymore. TKIP is deprecated in the 802.11-2012 standard.

IEEE 802.11i / WPA-2

WPA2 is the replacement for WPA and is based on the IEEE 802.11i (ratified) standard. Certification began in 2004, and from March 13, 2006, it was mandatory for all devices if you wanted to use the Wi-Fi trademark. The most significant upgrade is that WPA2 uses AES-CCMP encryption instead of the old RC4 encryption that WEP and WPA use.

For backward compatibility reasons, you can still use TKIP as a fallback mechanism for WPA clients.

WPA2 also introduced Wi-Fi Protected Setup (WPS). If you want to connect to a network that uses a pre-shared key, then you need to know the SSID and the pre-shared key.

With WPS, you only have to push a button or enter a PIN code, and your wireless client automatically configures the SSID and pre-shared key. WPS makes it easier for non-tech savvy users to configure a wireless network, especially when you use long, complex pre-shared keys.

Counter Mode Cipher Block Chaining Message Authentication Code Protocol (Counter Mode CBC-MAC Protocol) or CCM mode Protocol (CCMP) is an encryption protocol designed for Wireless LAN products that implements the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM mode) of the Advanced Encryption Standard (AES) standard.

WPS (WIFI PROTECTED SETUP)

WPS stands for WiFi Protected Setup and it was designed to make it as easy as possible for devices to join a wireless network. There are a couple of different methods that are used with WPS, but the most common one is the 'push button' method.

For example, most routers today will have a physical WPS button that you can press. Let's say that you have a printer which also has a WPS button, so to connect this wireless printer to your WiFi network you would press the WPS button on your WiFi router and within 2 minutes you would press the WPS button on your printer. This would initiate a connection process and your printer would connect to the Wi-Fi router in a few seconds. Another method is to use a WPS pin number during the WPS connection process.

WPS is the easiest way to join a wireless network and a lot of manufactures have built their wireless products with WPS. There's one more method - the Access Control or in some routers it's called the MAC Filter. MAC filtering is a security method based on access control. In this each address is assigned a 48-bit address which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices which you need on your Wi-Fi and the list of denied devices which you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way we can blacklist or white list certain computers based on their MAC address.

MAIN THREATS TO WI-FI SECURITY

As the internet is becoming more accessible, via mobile devices and gadgets, data security is becoming a top concern from the public, as it should be. Data breaches and security malfunctions can cost individuals and businesses thousands of dollars.

It is important to know the threats that are most prevalent in order to be able to implement the proper security measures.

MAN-IN-THE-MIDDLE ATTACKS

A man-in-the-middle (MITM) attack is an incredibly dangerous type of cyber attack that involves a hacker infiltrating a private network by impersonating a rogue access point and acquiring login credentials.

The attacker sets up hardware pretending to be a trusted network, namely Wi-Fi, in order to trick unsuspecting victims into connecting to it and sending over their credentials. MITM attacks can happen anywhere, as devices connect to the network with the strongest signal, and will connect to any SSID(Service Set Identifier or your network ID) name they remember.

CRACKING AND DECRYPTING PASSWORDS

Cracking and decrypting passwords is an old method that consists of what is known as “A brute force attack.” This attack consists of using a trial and error approach and hoping to eventually guess correctly. However, there are many tools that hackers can use to expedite the process.

Luckily, you can use these same tools to try and test your own network’s security. Software like John the Ripper, Nessus, and Hydra

PACKET SNIFFERS

Packet sniffers are computer programs that can monitor traffic on a wireless network. They can also intercept some data packages and provide a user with their contents. They can be used to harmlessly gather data about traffic, but in the wrong hands can introduce errors and break down a network.

HOW TO ENHANCE YOUR HOME WIRELESS NETWORK SECURITY

Step 1. Change the name of your default home network

If you want to better secure your home network, the first thing you should do is to change the name of your Wi-Fi network, also known as the SSID (Service Set Identifier).

Step 2. Make sure you set a strong and unique password to secure your wireless network

You probably know that every wireless router comes pre-set with a default username and password, which is needed in the first place to install and connect your router. The worst part: it's easy for hackers to guess it, especially if they know the manufacturer. So, make sure you change them both immediately. A good wireless password should be at least 20 characters long and include numbers, letters, and various symbols.

Step 3. Increase your Wi-Fi security by activating network encryption

Wireless networks come with multiple encryption languages, such as WEP, WPA, or WPA2. To better understand this terminology, WPA2 stands for Wi-Fi Protected Access 2 and is both a security protocol and a current standard in the industry (WPA2 networks are almost everywhere) and encrypts traffic on Wi-Fi networks.

Step 4. Turn off the wireless home network when you're not at home

In order to secure your network, we strongly recommend you disable the wireless home network, in case of extended periods of non-use.



Step 5. Change your default IP address on the Wireless router

Changing the default IP address to a less common one is another thing you should consider doing to better secure your home network and make it more difficult for hackers to track it.

Step 6. A firewall can help secure your Wi-fi network

Firewalls aren't just software programs used on your PC, they also come in the hardware variety. A hardware firewall does pretty much the same thing as a software one, but its biggest advantage is that it adds one extra layer of security. The best part about hardware firewalls is that most of the best wireless routers have a built-in firewall that should protect your network from potential cyber-attacks.

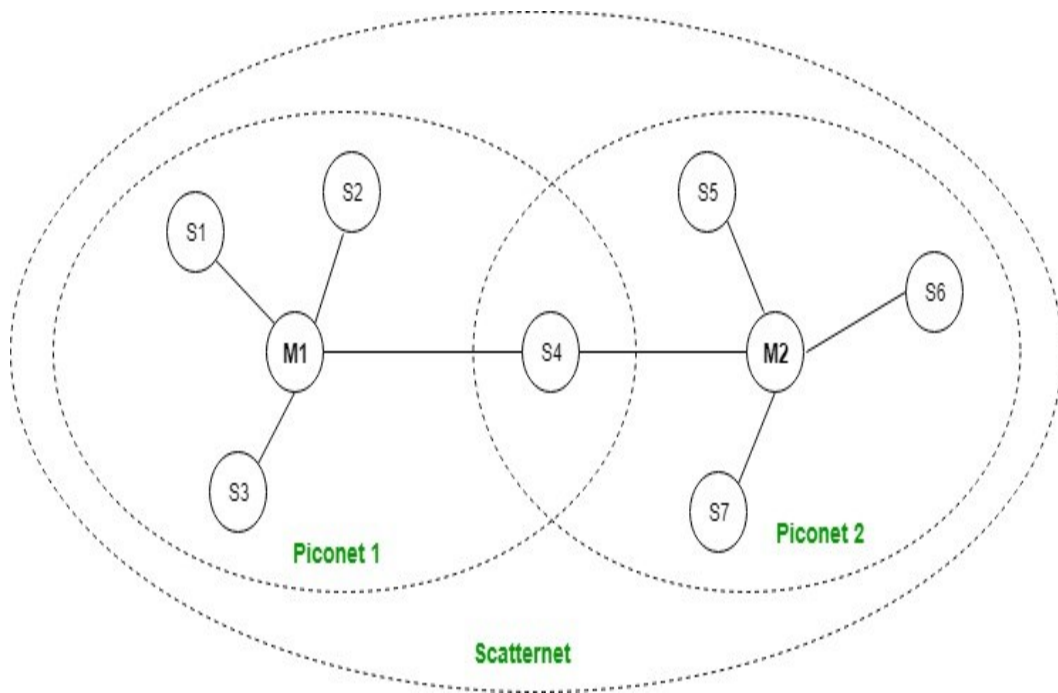
BLUETOOTH

Bluetooth is a short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz, and building personal area networks (PANs).

It was originally conceived as a wireless alternative to RS-232 data cables. It is mainly used as an alternative to wire connections, to exchange files between nearby portable devices and connect cell phones and music players with wireless headphones. In the most widely used mode, transmission power is limited to 2.5 milliwatts, giving it a very short range of up to 10 meters (30 feet).

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 35,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard.

BLUETOOTH ARCHIECTURE



Bluetooth technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A bluetooth network is called piconet and a collection of interconnected piconets is called scatternet.

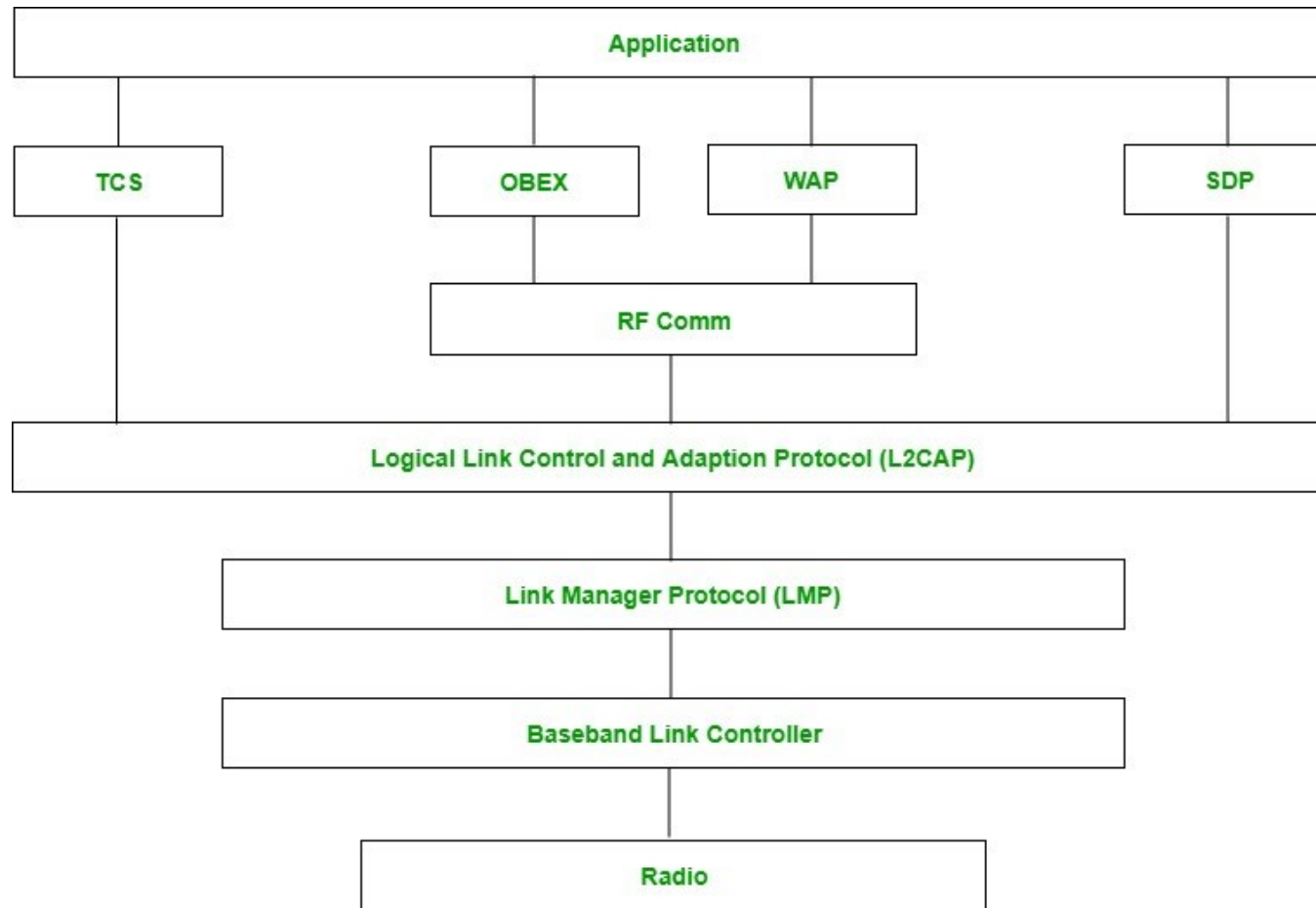
Piconet:

Piconet is a type of bluetooth network that contains one primary node called master node and seven active secondary nodes called slave nodes. Thus, we can say that there are total of 8 active nodes which are present at a distance of 10 metres. The communication between the primary and secondary node can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also have 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

Scatternet:

It is formed by using various piconets. A slave that is present in one piconet can be act as master or we can say primary in other piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.

BLUETOOTH PROTOCOL STACK



1. Radio (RF) layer:

It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of bluetooth transceiver. It defines two types of physical link: connection-less and connection-oriented.

2. Baseband Link layer:

It performs the connection establishment within a piconet.

3. Link Manager protocol layer:

It performs the management of the already established links. It also includes authentication and encryption processes.

4. Logical Link Control and Adaption protocol layer:

It is also known as the heart of the bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation and multiplexing.

5. SDP layer:

It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device.

6. RF comm layer:

It is short for Radio Frontend Component. It provides serial interface with WAP and OBEX.

7. OBEX:

It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

8. WAP:

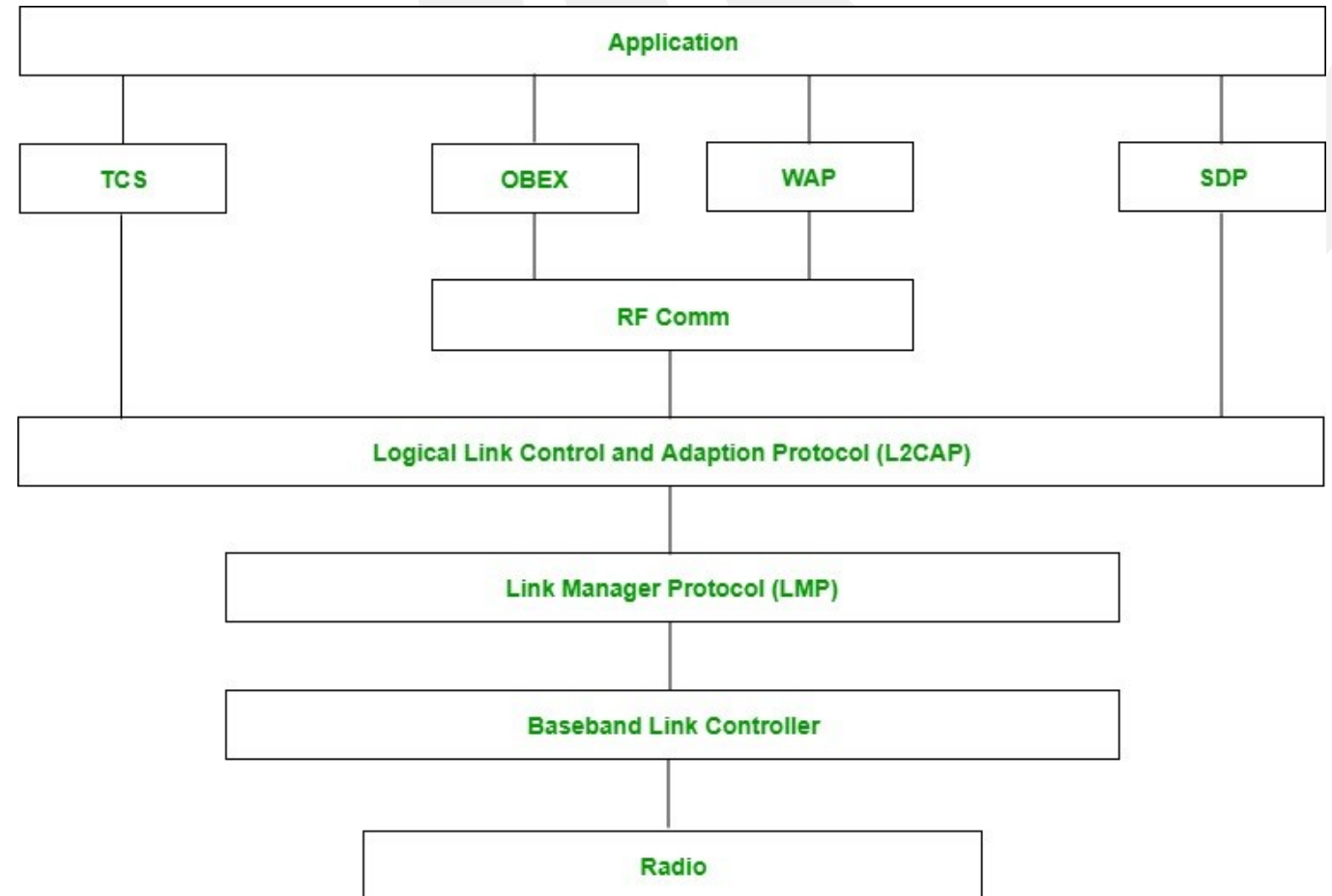
It is short for Wireless Access Protocol. It is used for internet access.

9. TCS:

It is short for Telephony Control Protocol. It provides telephony service.

10. Application layer:

It enables the user to interact with the application.





Advantages:

1. Low cost.
2. Easy to use.
3. It can also penetrate through walls.
4. It creates an adhoc connection immediately without any wires.
5. It is used for voice and data transfer.

Disadvantages:

1. It can be hacked and hence, less secure.
2. It has slow data transfer rate: 3 Mbps.
3. It has small range: 10 meters.

TYPES OF BLUETOOTH ATTACKS

Hackers can access a device by using several techniques, such as:

Bluebugging.

Bluebugging is a type of a Bluetooth attack through which hackers can access a device and eavesdrop on phone calls, connect to the Internet, send and receive text messages and emails, and even make calls (while the owner is unaware of it). It is usually associated with older phone models.

Bluejacking.

Bluejacking was once used for making pranks on people. It's the most common type of Bluetooth attack and is rather harmless and childish because a hacker can only send spam in the form of text messages to the hacked device. Bluejacking doesn't give hackers access to your smartphone or the data on it. Keep your Bluetooth settings to non-discoverable or invisible, or just ignore the messages you receive.

Bluesnarfing.

Hackers can perform a bluesnarfing attack on devices when they are within 300 ft (around 90 meters). This is one of the most dangerous Bluetooth attacks because, even if your device is in a non-discoverable mode, hackers can attack it and gain access to all the personal information in your device. They can copy all the content on your device, including your pictures and videos, phone number, contact list, emails, and passwords. However, the invisible mode makes it more difficult for hackers to figure out the model and name of your device.

Car whisperer.

The attack takes advantage of a common flaw in Bluetooth vehicle implementation wherein certain car manufacturers use the same 1234 or 0000 passkeys for authentication and encryption. Hackers can use a laptop and a Bluetooth antenna to connect and listen in on hands-free conversations or talk directly to the people in the car. Secure your car's audio, Bluetooth headset, and entertainment system by changing the manufacturer's PIN code.

Location tracking.

A Bluetooth attack used for locating and tracking devices. Those usually prone to this attack are fitness enthusiasts because their fitness wearables are always connected to their Bluetooth.

BlueBorne.

To perform a BlueBorne attack, hackers need to infect your device with malware. That will allow an attacker to take control of the device. What makes things even worse is that, once your device is infected, it can infect other devices it connects to. If your device's software is outdated and doesn't use a VPN, it is vulnerable to BlueBorne attacks.

A decorative graphic consisting of several concentric, light gray circular arcs that sweep across the upper right portion of the slide.

Hackers can be motivated to hack Bluetooth enabled devices for various reasons that may include:

- Accessing personal data and demanding blackmail or a ransom
- Eavesdropping on communications like phone calls and texts
- Infecting a device with malware to steal credentials
- Stealing financial information (e.g., PayPal login information or Tax returns)

BLUETOOTH SECURITY

Bluetooth security supports authentication and encryption. These features are based on a secret link key that is shared by pair of devices. A pairing procedure is used when two devices communicate for the first time to generate this key. There are three security modes to a device:

Mode 1 (non-secure)

This mode is non-secure. The authentication and encryption functionality is bypassed and the device is susceptible to hacking. Bluetooth devices operation in Bluetooth Security Mode 1. Devices operating like this do not employ any mechanisms to prevent other Bluetooth-enabled devices from establishing connections. While it is easy to make connections, security is an issue.

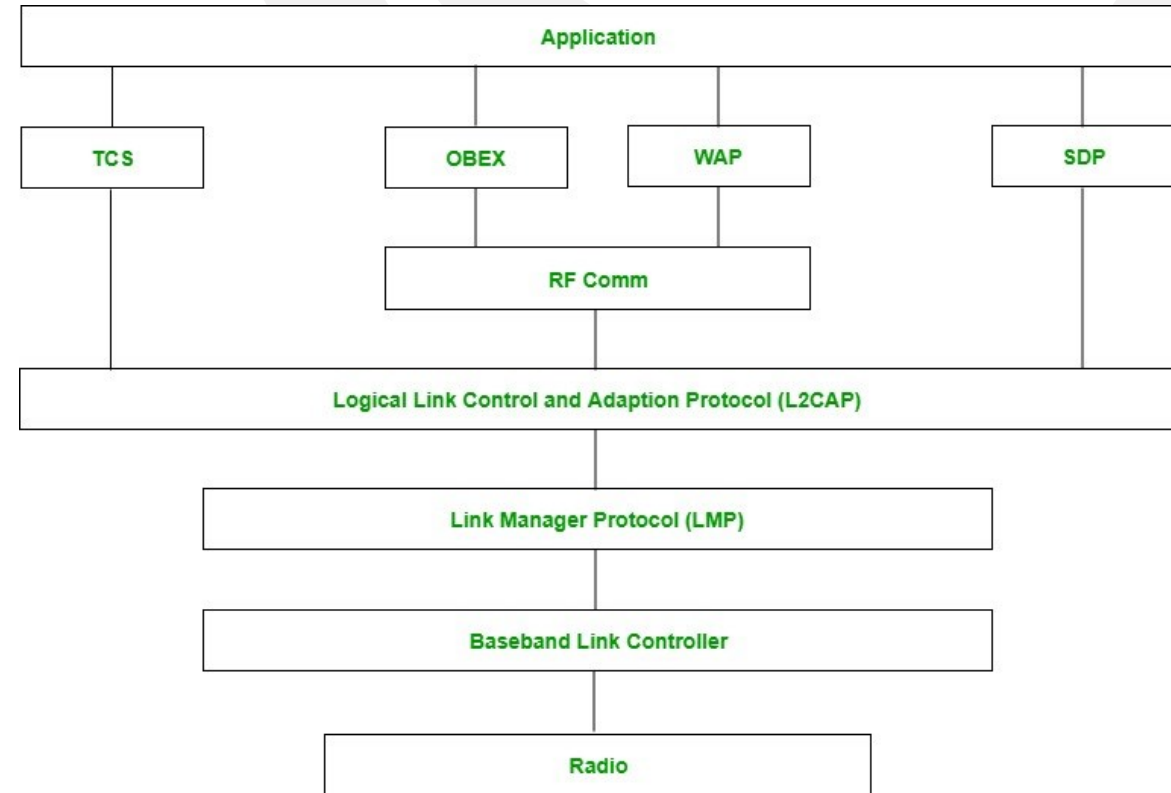
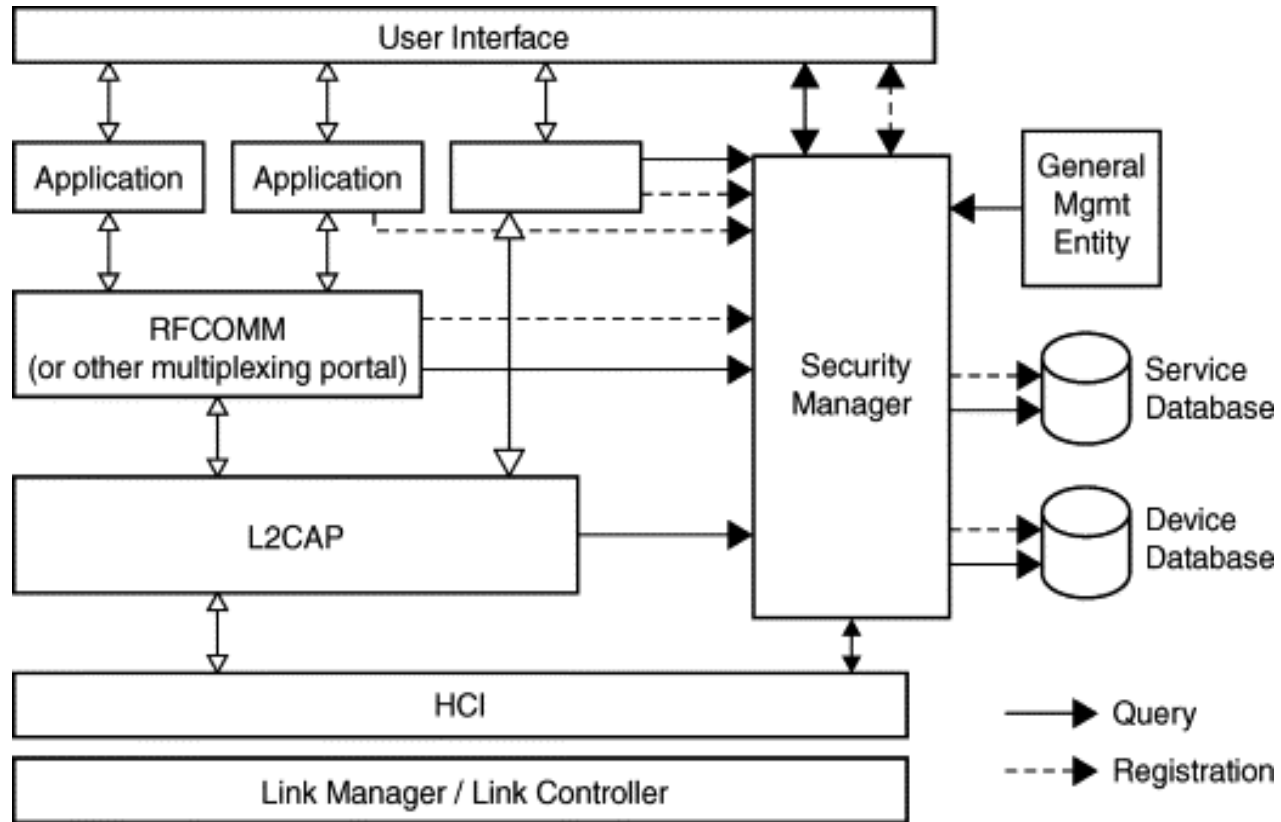
Mode 2 (Service level enforced security.)

A device does not initiate security procedures before channel establishment at the L2CAP level. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel.

Mode 3 (Link level enforced security.)

A device initiates security procedures before the link set-up at the LMP is completed.

BLUETOOTH SECURITY ARCHITECTURE

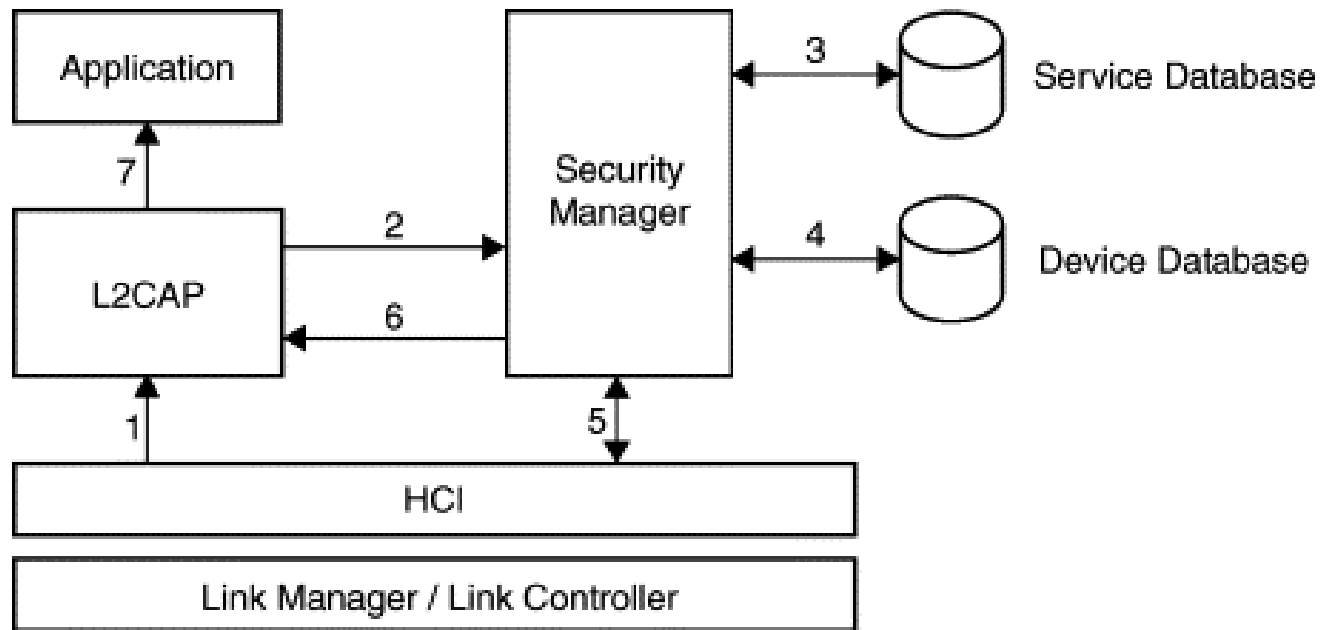


SECURITY LEVELS

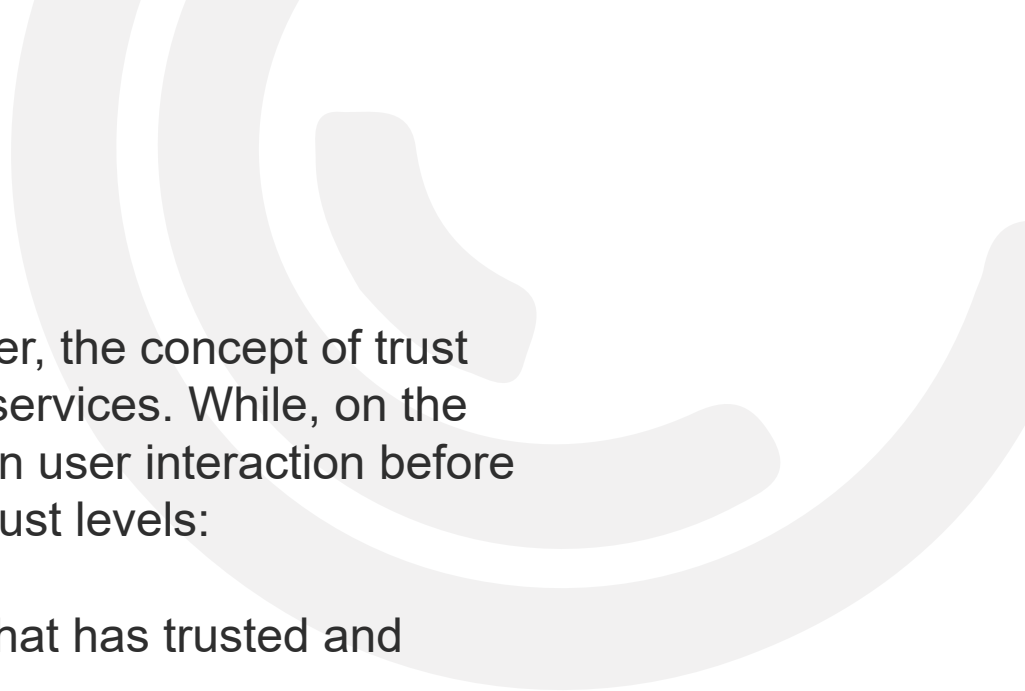

There are two kinds of security levels: authentication and authorization.

Authentication verifies who is at the other end of the link. In Bluetooth this is achieved by the authentication procedure based on the stored link key or by the pairing procedure. To meet different requirements on availability of services without user intervention, authentication is performed after determining what the security level of the requested service is. Thus, authentication cannot be performed when the ACL link is established. The authentication is performed when a connection request to a service is submitted. The following procedure is used

Authentication can be performed in both directions: client authenticates server and vice versa.

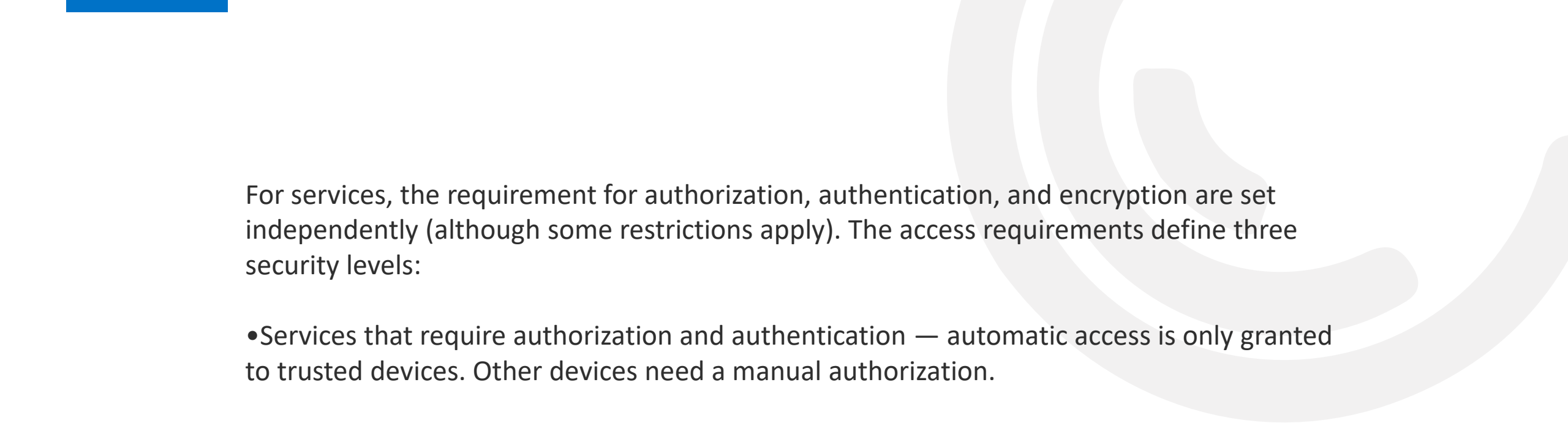


1. The connect request to L2CAP is sent.
2. L2CAP requests access from the security manager.
3. The security manager enquires the service database.
4. The security manager enquires the device database.
5. If necessary, the security manager enforces the authentication and encryption procedure.
6. The security manager grants access, and L2CAP continues to set up the connection.



Authorization. When one device is allowed to access the other, the concept of trust comes into existence. Trusted devices are allowed access to services. While, on the contrary, untrusted devices may require authorization based on user interaction before access to services is granted. There are two kinds of device trust levels:

1. *Trusted device*: A device with a fixed relationship (paired) that has trusted and unrestricted access to all services.
2. *Untrusted device*: This device has been previously authenticated, a link key is stored, but the device is not marked as trusted in the device database.
3. *An unknown device* is also an untrusted device. No security information is available for this device.



For services, the requirement for authorization, authentication, and encryption are set independently (although some restrictions apply). The access requirements define three security levels:

- Services that require authorization and authentication — automatic access is only granted to trusted devices. Other devices need a manual authorization.
- Services that require authentication only — authorization is not necessary.
- Services open to all devices — authentication is not required, no access approval is required before service access is granted.

A default security level is defined to serve the needs of legacy applications. This default policy will be used unless other settings are found in a security database related to a service.

LIMITATIONS OF BLUETOOTH SECURITY

Only a device is authenticated, and not its user.

There is no mechanism to preset authorization per service. However, a more flexible security policy can be implemented with the present architecture without a need to change the Bluetooth protocol stack.

Also, it is not possible to enforce unidirectional traffic.

TIPS ON SAFE BLUETOOTH USAGE

1	The 'discoverable' mode on your device is only meant to be used to "pair" two Bluetooth-enabled devices. When the pairing process is done, the 'discoverable' mode can be turned off as the devices should remember each other.
2	Refrain from communicating or transmitting sensitive and personal information using the Bluetooth-enabled device as it might be sniffed.
3	Use strong passkey that is randomly generated when pairing Bluetooth devices and never enter passkeys when unexpectedly prompted for them.
4	Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
5	Avoid accepting attachments or applications received on your phone or device if you were not expecting it no matter how legitimate it may be. If your device asks to pair and you didn't initiate the pairing, deny it and check that your 'discoverable' setting is set to 'off' or 'hidden'.