Name: Vishal Pote
Topic: Wireless Security:

Wireless technologies will affect our lives in more and more ways every year. Have a look at the sample statistics that have been found. Some of them seems to be a scary, but at the same time they simply show how much we rely on wireless communication nowadays.

By 2020, around 24 Billion devices will be connected to the internet, with more than half connected via wireless. This is true Internet of Things (IoT). How does it sound, taking into a fact that we have around 7.4 Billion people living on the earth now?
About 70% of all the types of wireless communication is Wi-Fi (802.11 standard).
The speed of the Wi-Fi network has grown from 802.11a - 54Mbps to Gbps.
Every day, millions of people are making cash transfer and accessing their bank account using smartphones over the Wi-Fi.So the need for wireless network is increasing day by day and security is big area of concern here.

Are we still hesitant about the importance of security in wireless implementations?

Wireless security is nothing but protecting computers, smartphones, tablets, laptops and other portable devices along
with the networks they are connected to, from threats and vulnerabilities associated with wireless computing.

When we think about wireless communication, we imagine some systems connected to antennas that speak together over the air using radio waves that are invisible to human eye. Honestly speaking, this is perfectly a true definition, but in order to break things (or rather you prefer the word "hack")you need to learn how all those concepts and architectures work together.Wireless communication refers to any type of data exchange between the parties that is performed wirelessly (over the air).
This definition is extremely wide, since it may correspond to many types of wireless technologies, like -

Wi-Fi Network Communication
Bluetooth Communication
Satellite Communication
Mobile Communication

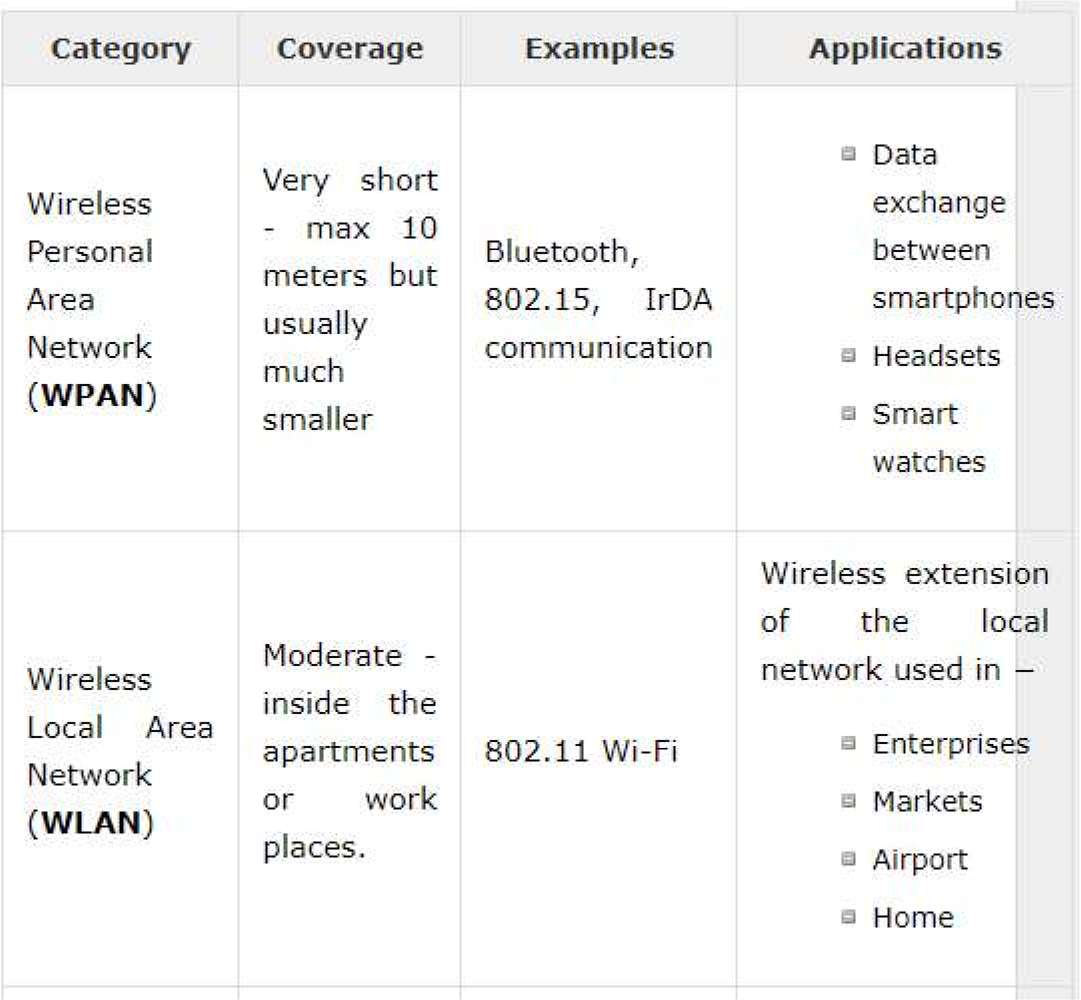
All the technologies mentioned above use different communication architecture, however they all share the same "Wireless Medium" capability.

What does Wireless Network Security mean?

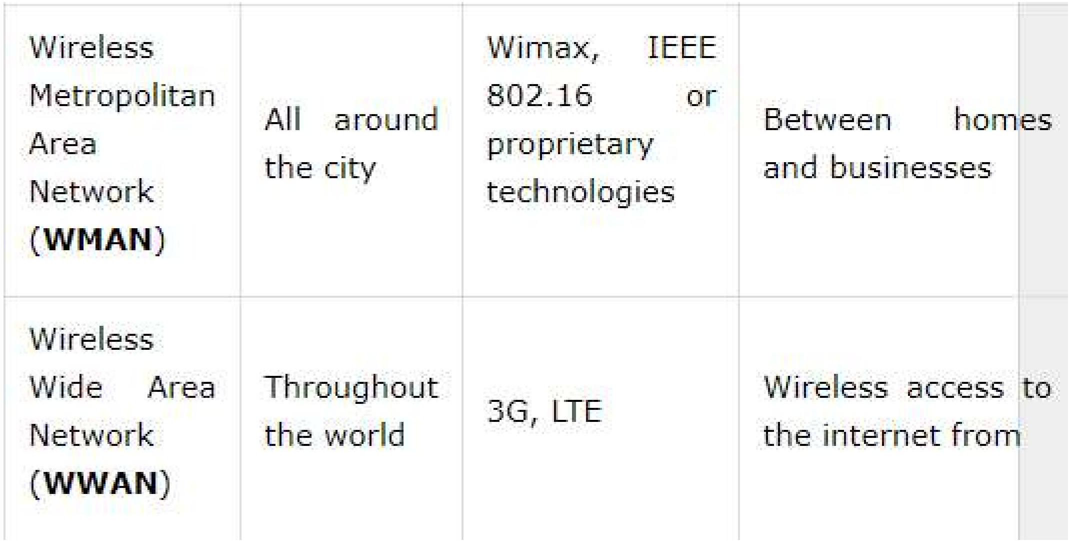
Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network. It is a subset of network security that adds protection for a wireless computer network.
Wireless network security is also known as wireless security.
Typically, wireless network security is delivered through wireless devices (usually a wireless router/switch)

that encrypts and secures all wireless communication by default. Even if the wireless network security is compromised,
the hacker is not able to view the content of the traffic/packet in transit. Moreover, wireless intrusion detection and prevention systems also enable protection of a wireless network by alerting the wireless network administrator in case of a security breach.

Wireless network may be classified into different categories based on the range of operation they offer. The most common classification scheme divides the wireless networks into four categories listed in the table below, together with short examples.



Category	Coverage	Examples	Applications
Wireless Personal Area Network (**WPAN**)	Very short - max 10 meters but usually much smaller	Bluetooth, 802.15, IrDA communication	▪ Data exchange between smartphones ▪ Headsets ▪ Smart watches
Wireless Local Area Network (**WLAN**)	Moderate - inside the apartments or work places.	802.11 Wi-Fi	Wireless extension of the local network used in – ▪ Enterprises ▪ Markets ▪ Airport ▪ Home



Wireless Metropolitan Area Network (**WMAN**)	All around the city	Wimax, IEEE 802.16 or proprietary technologies	Between homes and businesses
Wireless Wide Area Network (**WWAN**)	Throughout the world	3G, LTE	Wireless access to the internet from

Wireless Security Wi-Fi Authentication Modes

Wireless Security Wi-Fi Authentication Modes

Open Authentication
The term Open Authentication is itself very misleading.
In plain English, what this exchange is saying is that, in authentication request the wireless client (supplicant) is saying "Hi AP, I would like to authenticate" and authentication response from the AP is stating "OK, here you go". Do you see any kind of security in this setup? Neither do I…

That is why, Open Authentication should be never used, since it simply allows any client to authenticate to the network, without the right security check.

Wireless Security - Encryption

In general, encryption is the process of transforming the data, into some kind of cyphertext that would be non-understandable for any 3rd party that would intercept the information. Nowadays, we use encryption every single day, without even noticing. Every time you access your web bank or mailbox, most often when you log in to any type of web page, or create a VPN tunnel back to your corporate network.

Some information is too valuable, not to be protected. And, to protect the information efficiently, it must be encrypted in a way that would not allow an attacker to decrypt it.

Types of Wireless Encryption
To start speaking about wireless encryption, it is worth saying that there are 2 types of encryption algorithms: Stream Cipher and Block Cipher.

Stream Cipher ? It converts plaintext into cyphertext in a bit-by-bit fashion.
Block Cipher ? It operates on the fixed-size blocks of data.

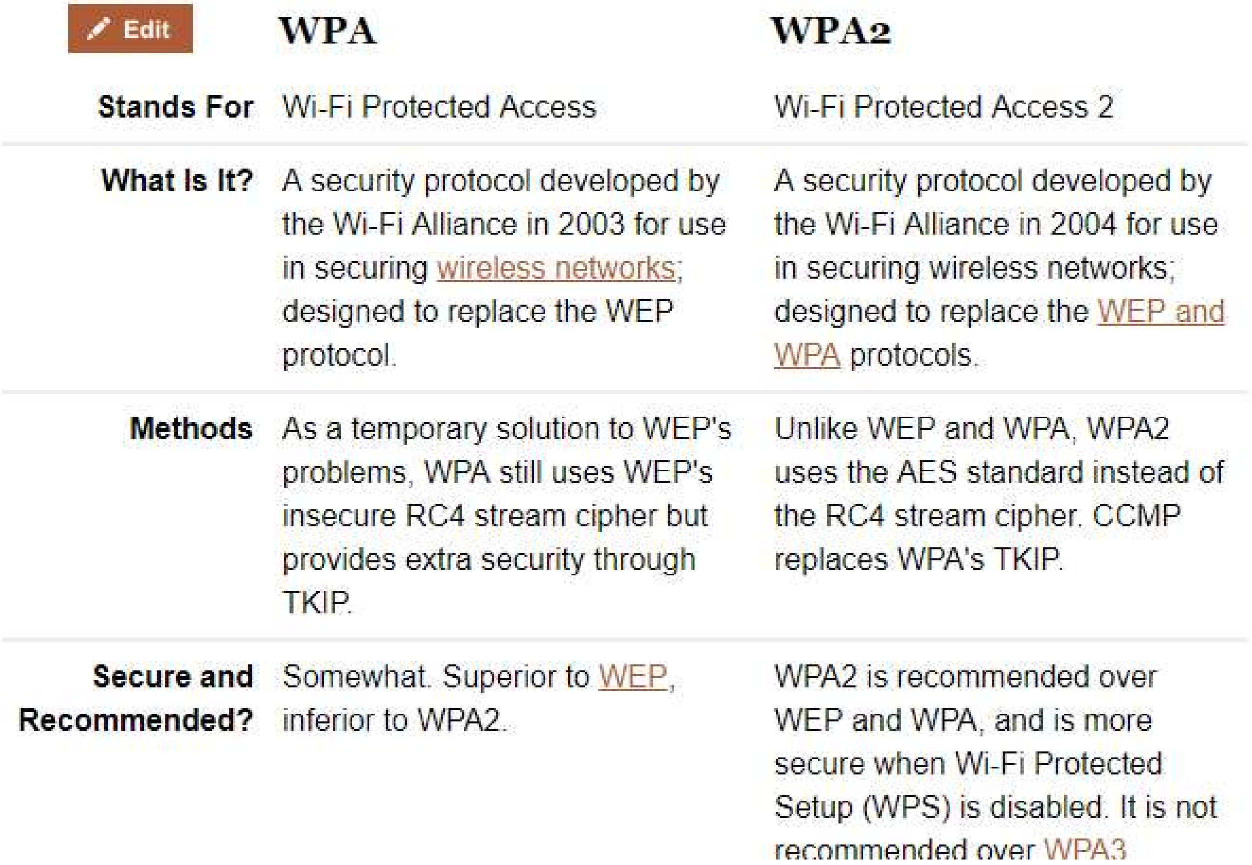
WEP vs WPA vs WPA2

WEP was the first wireless "secure" model that was supposed to add authentication and encryption. It is based on RC4 algorithm and 24 bits of Initialization Vector (IV). This is the biggest drawback of the implementation that leads to WEP being crack able within a few minutes, using the tools that anyone can have installed on their PCs.

In order to enhance the security, WPA2 was invented with strong encryption model (AES) and a very strong authentication model based on 802.1x (or PSK). WPA was introduced just as a staging mechanism for smooth transition to WPA2. A lot of wireless cards did not support the new AES (at that time), but all of them were using RC4 + TKIP. Therefore WPA was also based on that mechanism, just with a few advancements.

Most wireless access points come with the ability to enable one of three wireless encryption standards: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) or WPA2. **WPA2** is more secure than its predecessor, WPA (Wi-Fi Protected Access), and should be used whenever possible. Wireless routers support multiple security protocols to secure wireless networks, including WEP, WPA and WPA2. Of the three, WPA2 is the most secure, as this comparison explains.

In 2018, the Wi-Fi Alliance released WPA3, which is now recommended over WPA2 but WPA3-certified hardware is not expected to be widely available until late 2019.



Edit	WPA	WPA2
Stands For	Wi-Fi Protected Access	Wi-Fi Protected Access 2
What Is It?	A security protocol developed by the Wi-Fi Alliance in 2003 for use in securing wireless networks; designed to replace the WEP protocol.	A security protocol developed by the Wi-Fi Alliance in 2004 for use in securing wireless networks; designed to replace the WEP and WPA protocols.
Methods	As a temporary solution to WEP's problems, WPA still uses WEP's insecure RC4 stream cipher but provides extra security through TKIP.	Unlike WEP and WPA, WPA2 uses the AES standard instead of the RC4 stream cipher. CCMP replaces WPA's TKIP.
Secure and Recommended?	Somewhat. Superior to WEP, inferior to WPA2.	WPA2 is recommended over WEP and WPA, and is more secure when Wi-Fi Protected Setup (WPS) is disabled. It is not recommended over WPA3

WPA3 is the next generation of Wi-Fi security and provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi CERTIFIED WPA2, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical networks. All WPA3 networks Use the latest security methods
Disallow outdated legacy protocols
Since Wi-Fi networks differ in usage purpose and security needs, WPA3 includes additional capabilities specifically for personal and enterprise networks. Users of WPA3-Personal receive increased protections from password guessing attempts, while WPA3-Enterprise users can now take advantage of higher grade security protocols for sensitive data networks.

WPA3, which retains interoperability with WPA2 devices, is currently an optional certification for Wi-Fi CERTIFIED devices. It will become required over time as market adoption grows.

WPA3-Personal
WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) in WPA2-Personal. The technology is resistant to offline dictionary attacks where an adversary attempts to determine a

network password by trying possible passwords without further network interaction.

Securing wireless access points: Wireless testing tools

NetStumbler - NetStumbler displays wireless access points, SSIDs, channels, whether WEP encryption is enabled and signal strength. NetStumbler can connect with GPS technology to accurately log the precise location of access points.

MiniStumbler - A smaller version of NetStumbler designed to work on PocketPC 3.0 and Pocket PC 2002 platforms. It provides support for ARM, MIPS and SH3 CPU types.

AirSnort - AirSnort is a wireless LAN (WLAN) tool which cracks WEP encryption keys. AirSnort passively monitors wireless transmissions and automatically computes the encryption key when enough packets have been gathered.

Kismet - Kismet is an 802.11 wireless network detector, sniffer, and intrusion detection system. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

SSID Sniff - A tool to use when looking to discover access points and save captured traffic. Comes with a configured script and supports Cisco Aironet and random prism2 based cards.

WifiScanner - WifiScanner analyzes traffic and detects 802.11b stations and access points. It can listen alternatively on all 14 channels, write packet information in real time, search access points and associated client stations. All network traffic may be saved in the libpcap format for post analysis.
Wireless packet analyzers, or sniffers, basically work the same way as wired network packet analyzers: they capture packets from the data stream and allow the user to open them up and look at, or decode, them. Some wireless sniffers don't employ full decoding tools but show existing WLANs and SSIDs.

Wireless Threats

Access Control Attacks:-

The concept of access control is all about controlling, who have access to the network, and who does not. It prevents malicious 3rd parties (unauthorized) from associating to the wireless network. The idea of access control is very similar to an authentication process; however, those two concepts are complementary. Authentication is most often based on a set of credentials (username & password) and access control may go beyond that and verify other characteristics of the client user or client user's device.

Very well-known access control mechanism used in wireless networks is based on MAC address whitelisting. The AP stores a list of authorized MAC addresses that are eligible to access the wireless network. With tools available nowadays, this security mechanism is not a very strong one, since MAC address (hardware address of the wireless client's chipset) may be spoofed very simply.

The only challenge is to find out what MAC addresses are allowed by AP to authenticate to the network. But since wireless medium is a shared one, anyone can sniff the traffic flowing through the air and see the MAC addresses in the frames with valid data traffic (they are visible in the header that is not encrypted).

Wireless Security - Confidentiality Attacks

The role of attacks targeting the confidentiality of the information, is simply to break the encryption model used in the wireless deployment. Looking at variety of security models in the field the following general recommendations may be put

No Encryption/ WEP Encryption These are not very secure approaches and should not be used under any circumstances.

TKIP Encryption This encryption model is used in WPA deployments. It has not yet been cracked, but TKIP is not considered as strong mean of encryption, due to the use of weaker RC4 algorithm.

CCMP Encryption This is used with WPA2. So far, it is considered the safest encryption model that is based on not-breakable AES algorithm.

The main goal of all kinds of attacks is to break the encryption and get a value of the key. This would give the attacker 2 things: broken confidentiality of other users and direct access to the wireless network.

Wireless Security - DoS Attack

The attacks which are directed at disabling the service (making the target not available) or degrading its performance (lowering the availability) lands under the umbrella of Denial of Service (DoS) attacks. The cost of such an attack may be very expensive for a victim or companies, whose business is based on e-commerce. They can count the costs of the attack in millions of dollars, depending on the length of their web service not being available.

Wireless networks are also playing a crucial part in productivity of the employees. We all use wireless laptops and smartphones in a workplace. With the lack of wireless network working, our productivity is decreased.

Rogue Access Point Attacks

When we think about corporate networks, the corporate WLAN is an authorized and secured wireless portal to the network resources. A rogue access device (AP) is any WLAN radio that is connected to the corporate network (most often to some network switch) without the authorization.

Most of the rogue access points that are installed by employees (malicious users or by mistake) are actually not the same AP's that the IT department in the organization is using, but some Small-office home-office (SOHO) wireless routers - the same ones, that you probably have at home. In the situation when they are misconfigured or configured without any security - it opens a next attack surface for having easy access to a very secure network).

If the network resources are exposed by a rogue access point, the following risks may be identified

Data Theft: Corporate data may be compromised.

Data Destruction:Databases may be erased.

Loss of Services : Network services can be disabled.

Malicious Data Insertion : An attacker may use a portal to upload viruses, key loggers or pornography.

3rd Party Attacks : A company's wired network may be used as a launching pad for 3rd party attacks against other networks across the internet.