**a) Vulnerabilities of the wireless networks:**

1. Accidental association: Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as accidental association. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s overlapping network, the user may not even know that this has occurred.
2. Malicious association: 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 . These types of laptops are known as «soft APs» and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans.
3. Ad-hoc networks: Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-topeer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.
4. Non-traditional networks: Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These nontraditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.
5. Man-in-the-middle attacks: A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP . Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network.
6. Denial of service: A Denial-of-Service attack occurs when an attacker continually bombards a targeted AP or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These attacks rely on the abuse of protocols such as the Extensible Authentication

Protocol .

1. Network injection: In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as «Spanning Tree» , OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs.
2. Identity theft (MAC spoofing): Occurs when a cracker is able to listen in on

network traffic and identify the MAC address of a computer with network privileges.

Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC IDs to gain access and utilize the network. However, a

number of programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

1. Caffe Latte attack: The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client.

**b) We can reduce the vulnerabilities of the wireless networks by taking these three steps:**

1. Eliminating rogue access points: The best method for dealing with the threat of rogue access points is to use 802.1x on the

wired network to authenticate all devices that are plugged into the network. Using 802.1x will

prevent any unauthorized devices from connecting to the network.

2. Properly configuring all authorized access points: Organizations also need to ensure that all authorized wireless access points are securely

configured. It is especially important to change all default settings because they are

wellknown and can be exploited by attackers.

3. Using 802.1x to authenticate all devices: Strong authentication of all devices attempting to connect to the network can prevent rogue

access points and other unauthorized devices from becoming insecure backdoors. The 802.1x

protocol discussed earlier provides a means for strongly authenticating devices prior to

assigning them IP addresses.

4. Training and Educating Users: Notice that Figure 1 also includes users as the fourth basic component of wireless

networking. As is the case with wired security, users are the key component to wireless

networking security. Indeed, the importance of training and educating users about

secure wireless behavior cannot be overstated. To be effective, user training and

education needs to be repeated periodically.

5. Securing Wireless Client Devices: Loss or theft of laptops and PDAs is a serious problem. laptops and PDAs

often store confidential and proprietary information. Consequently, loss or theft of the

devices may cause the organization to be in violation of privacy regulations involving

the disclosure of personal identifying information it has collected from third parties.

6. Use of Encryption: The most effective way to secure your wireless network from intruders is to encrypt, or

scramble, communications over the network. Most wireless routers, access points, and base

stations have a built-in encryption mechanism. If your wireless router doesn’t have an

encryption feature, consider getting one that does. Manufacturers often deliver wireless

routers with the encryption feature turned off. You must turn it on.

7. Use anti-virus and anti-spyware software, and a firewall: Computers on a wireless network need the same protections as any computer connected to

the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your

firewall was shipped in the “off” mode, turn it on.

8. Allow only specific computers to access your wireless network: Every computer that is able to communicate with a network is assigned its own unique

Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow

only devices with particular MAC addresses access to the network. Some hackers have

mimicked MAC addresses, so don’t rely on this step alone.

9. Turn off your wireless network when you know you won’t use it: Hackers cannot access a wireless router when it is shut down. If you turn the router off

when you’re not using it, you limit the amount of time that it is susceptible to a hack.

10. Network Auditing: Wireless network auditing is an important part of WLAN security policy. The network

needs to be regularly audited for rouge hardware. In this method the network is scanned and

mapped for all access points and WLAN nodes. Then this is compared with previous network

map. Commonly available network mapping tools like netstumbler and wavelan-tool can be

used to do this. Specialized tools such as Airsnort can be used for WEP cracking and auditing

the network for weak keys, key reuse and WEP security settings. These methods include the

same tests as those carried out by hackers for breaking into the network.

**c) Recent wireless attack:**

As per scientists at IoT security firm Armis that found the assault vector, the purported "BlueBorne" assaults can hop starting with one adjacent Bluetooth gadget then onto the next remotely. It assesses that there are 5.3 billion gadgets in danger.

"Whenever misused, the vulnerabilities could empower an aggressor to assume control over gadgets, spread malware, or set up a 'man-in-the-center' to access basic information and systems without client connection," as per the organization. "The assault does not require the focused on gadget to be matched to the aggressor's gadget, or even to be determined to discoverable mode… since the Bluetooth procedure has high benefits on every working framework, misusing it gives for all intents and purposes full command over the gadget."

As a feature of a planned exposure, Armis said Google and Microsoft have officially made patches accessible to their clients.

In an announcement to Threatpost, Microsoft stated: "Microsoft discharged security refreshes in July and clients who have Windows Update empowered and connected the security refreshes, are ensured consequently. We refreshed to secure clients at the earliest opportunity, however as a dependable industry accomplice, we retained exposure until different merchants could create and discharge refreshes."

Microsoft's September Patch Tuesday divulgence records one of the BlueBorne bugs (Bluetooth driver satirizing weakness – CVE-2017-8628) as a major aspect of its security patches for the month.

Apple iOS gadgets running the latest adaptation of the OS (10.x) are sheltered, Armis said.

As per scientist, just 45 percent of Android telephones (960 million) are patchable, leaving 1.1 billion dynamic Android gadgets more established than Marshmallow (6.x) defenseless.