Wireless Network Vulnerabilities and Attacks

- There is has been a huge increase in the deployment of wireless networks both in the workplace and in homes simply due to the fact that they provide organizations and users with three primary benefits:

  - Portability and flexibility
  - Increased productivity
  - Lower installation costs.

- In addition, Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices.

- All this convenience and flexibility however brings with it considerable risks and network vulnerabilities.

- Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new.

- Perhaps the most significant source of risks in wireless networks is that the technology’s underlying communications medium, the radio channel, is open to intruders, making it the logical equivalent of an open Ethernet port in the parking lot.

- The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications.

- Unauthorized users may gain access to systems and information, corrupt the important data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use the resources to launch attacks on other networks.

- There is a widespread lackadaisical attitude when it comes to wireless security; most people will suggest that they have nothing to hide and therefore they don’t really care of someone sniffs their wireless channels.

- However, everyone should be concerned if attackers intrude into their networks, delete or steal sensitive information, plant viruses, and worse yet, use their systems to launch attacks on other networks.

Wireless Attack Scenarios

- We will go through some possible scenarios where wireless network vulnerabilities can be exploited and the ramifications of such compromises.

- **Hotels**
  - Many hotels nowadays make wireless network service available to their guests and in almost all cases these are open to anyone within range.
  - It is relatively easy to place an AP on a hotel network or authenticate with an existing AP.
  - With an open network, packets can bi sniffed, and passwords and other sensitive information can be captured.
  - In the worst case, depending on how the hotel is using its wireless infrastructure, essential systems such as alarms, elevators, cameras, etc., can now be controlled by an attacker from anywhere within range of the APs.
  - This is effectively allowing someone from off the street to access a workstation connected to the hotel network.

- **Hospitals and other Medical Facilities**
  - Attackers can sniff network traffic and glean very sensitive patient data.
  - This could be used to blackmail people or spread malicious gossip.
  - More worrisome is the potential for someone to intrude on the network and change medication information and/or medical data.
  - Imagine a truly frightening scenario medical facilities and equipment are made unavailable due to a network compromise, and lives are at stake.

- **Espionage**
  - An attacker can park themselves within the coverage areas of corporations and government organizations and sniff data from wireless traffic and are able to get proprietary and sensitive data.
  - Corporate offices or Mobile Hotspots (i.e.: Starbucks & airports) are very popular places to sniff network traffic.

- **Blackmail or Character Assassination**

- An attacker will find and authenticate with a residential users’ AP with the express purpose of using the victims AP (and therefore the IP) to send or download incriminating information.

- The attacker or blackmailer will log onto a web-based email service and emails an attachment containing child pornography.

- Next, the blackmailer places child pornography on the victims’ computer. The IP address is traced to the victim and a search and seizure will be almost inevitable.

- The same attack can be extended to corporate networks with equally unpleasant results.

Types of Wireless Network Attacks

- The techniques for attacking wireless network are not new; they are based mostly on traditional attacks used on wired networks.

- The one main difference is that the main objective behind a wireless attack is not necessarily to compromise the wireless network itself, but to establish a beachhead into the network within.

- Given that traditional, wired networks have been around for many years now and have developed very effective and hardened methods of defense, attackers are now focusing on the one weakness in the perimeter, and that is the wireless AP.

- Network security attacks are typically divided into **passive** and **active** attacks. These two broad classes are then subdivided into other types of attacks.

Passive Attack

- This is an attack in which an unauthorized party gains access to wireless network traffic but in a non-intrusive way so that the frame contents are not modified (i.e., eavesdropping).

- A passive attack is very difficult to detect simply due to the fact that the attacker is not affecting the traffic flow in any way.

- Passive attacks can be either **eavesdropping** or **traffic analysis** (sometimes called traffic flow analysis).

- **Eavesdropping**
    - The attacker monitors transmissions for important message content.
    - An example of this attack is a person listening into the transmissions on a LAN and identifying items of interest such as email addresses, user names, passwords, destination URLs, etc.

- **Traffic analysis**
    - This involves much more effort and perseverance on the attackers part because the main objective is collect as many frames as possible over a large period of time and then perform some sort of analysis on the information that is gathered.
    - The type of analysis will depend on the tool being used. This can go from simply identifying APs (BSSIDs), their locations (using GPS), signal strengths, etc., to much more complex analysis such as cracking the WEP keys.

<u>Active Attacks</u>

- An attack whereby an attacker intrudes into the network and makes modifications to a message, data stream, or file.
- It is possible to detect this type of attack but it may not be preventable. Active attacks may be categorized into four general types (or combination thereof):
- **Masquerading**
    - The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
- **Replay**
    - The attacker monitors transmissions (passive attack) and then retransmits messages as the legitimate user.
- **Message modification**
    - The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service**
    - The attacker prevents or prohibits the normal use or management of communications facilities.

- Most attacks associated with 802.11 are a combination and/or variation on the above broad categories.

Reconnaissance

- As always, the first step in the attack process is to perform as much reconnaissance as is necessary to acquire all the information that will allow an attacker to successfully attack and compromise a wireless network.

- The first phase of wireless reconnaissance is to look for the obvious signs of wireless devices and system components:

- **Antennae**
    - These would be located on walls, ceilings, hallways, roofs and windows

- **Access Points**
    - Usually located on walls, ceilings, support beams, shelves and of course, desks

- **Network Cables**
    - Traveling up walls, cabling trays, or across ceilings

- **Devices – Scanners/PDAs**
    - Employees, reception or checkout areas

- Once an attacker has located the presence of wireless APs, the next step is to determine whether or not connection can be established with the AP.

- In many cases finding obvious signs of the presence of wireless networks is not possible simply due to the fact that physical access to the premises is not possible.

- When physical surveillance is too difficult or impossible, then a very effective alternative is “war driving”.

War Driving

- Back in ancient times when dial-up modems were en vogue, and corporate networks had their own pools of modems, attackers would use a technique called "war-dialing" in which scripts would generate large blocks of random phone numbers and dial them, attempting to find a phone that would answer with a modem connection string.

- This sort of mass dialing transferred itself onto the Internet once the latter became the prevalent way of accessing information and computers, and it became even more common and even more effective by allowing attackers to not even need a phone line to knock on the doors of groups of computers, found by randomly generating their IP address.

- Now we have a situation where wireless networks have suddenly become the target of "war drivers."

- Using special software, a global positioning system (GPS) unit, and a notebook computer with wireless capabilities, an attacker can drive through any city or populated area, sampling the airwaves for wireless access points.

- The special war driving software keeps information about latitude, longitude, and configuration of the access points found along the driver's route.

- In fact, one can travel the sky train (say from Burnaby to Vancouver) with a laptop and find plenty of access points that are open with no security enabled.

- One of the best war driving applications is called **NetStumbler**, and is available free of charge for both the Linux and Windows platforms.

- War driving has become a very popular pastime among hobbyists; participants of this activity assemble their rigs of hardware and software with the intent of cruising streets to find wireless access points and then share the information widely.

- A “**rig**” refers to all of **the hardware and software components** that are used to carry out a wardriving exercise.

- **Computer System**

    - Most wardrivers choose to use either a laptop or PDA since these devices are relatively light and portable and they will function for long periods of time on battery power.

    - A simple power inverter may be used with the cigarette lighter adaptor found in most vehicles to provide power for the entire rig.

- **Wireless Cards**

    - The next necessary component of a wardriving rig is a wireless LAN card.

    - The most important specification of a wireless LAN card is the chipset that the wireless card contains.

    - Three major chipsets are used in 802.11b wireless LAN cards that support wardriving:

        - Hermes: Lucent, Dell, IBM, Sony
        - Prism: Intel, Linksys, NetGear, Proxim, SMC, UsRobtics, Zoom
        - Aironet: Cisco

    - It is important to select the wireless LAN card since some software will only support a particular 802.11 chipset.

- Another important characteristic to consider for a wireless LAN cards is whether or not they have an external antenna connector.

- Some cards have dual external antenna connectors, which makes it a very powerful general purpose receives.

- We can connect two antennae to the ports, for example, a combination of two directional antennae will provide scanning abilities on both sides of a street while wardriving.

- **External Antennae**
  - External antennas are essential in any wardriving activity; they can be used to extend the range of a wireless LAN card and will allow one to detect more wireless access points with less distance traveled.
  - Attaching an external antenna to a wireless LAN card will require the use of a cable called a "**pigtail".**
  - A pigtail is usually a short 40 to 80 cm cable that converts connectors from the wireless LAN card's proprietary connector (usually MMCX) to a standard antenna connector (N type).
  - An N-male connector is usually used for the other end of the pigtail and it connects with the N-female cable of the antenna.
  - The types of antenna that can be used here are: directional and omni-directional.
  - Directional antennas tend to be less popular unless targeting a very small area, since they focus the radio wave transmission and reception in one specific direction.
  - An omnidirectional antenna is a much popular choice since it will pick up APs in a wide geographical area.

- **Amplifiers**
  - Most wireless cards, combined with a 15dBi omni-directional antenna, will achieve power levels very close to the 1-watt regulatory limit.
  - However, in some cases in may be necessary to use a 1 watt amplifier to overcome signal loss produced by long cables and multiple cable connectors.

- **GPS Devices**

  - Data collected from a wardriving session would not be complete without also recording the geographic location of the wireless access point.

  - Collection of the AP coordinates has become automated with the use of common GPS devices.

  - Most GPS devices come equipped with a serial cable that can be attached to a laptop or PDA, therefore wireless network scanning software may have access to the GPS data.

  - Any GPS device that is capable of NMEA output through the serial port will be compatible with most wireless network scanning programs.

- The typical configuration for a wardriving rig is to place the laptop in the passenger-side seat, place the GPS unit on the dashboard and to magnetically-mount the external antenna to the top of the car.

- Several strategies can be employed to maximize the number of wireless access points detected.

- It is important to keep as low a profile as possible and not to become too conspicuous.

- One common sense strategy is to avoid backtracking down streets that have already been driven through.

- Densely populated areas with higher than average household incomes are ideal wardriving targets in the suburbs.

- In urban areas schools, hotels, retail businesses and corporate offices are likely to have multiple wireless access points.

- As far as the driving speed is concerned, it must be noted that the average GPS device will only update every second and it takes Kismet about 4 seconds to hop through all of the channels of the 802.11b protocol.

- NetStumbler on the other hand will quickly detect wireless access points because it is actively seeking access points and utilizing the 802.11b protocol that aids in the quick discovery of access points

- **Mapping**

- It is very useful to present all of the wardriving data in a visual form that is easy to understand.

- The current standard for doing this is to plot all of the wireless access points on a map and to color the markers red for WEP encrypted and green for no encryption.

- There a few websites exist that allow wardrivers to upload access point information and locations.

- This data is compiled into a master list and plotted on a map in real time.

Detecting Wardrivers

- There are a couple ways in which wardriving activity can be detected. Keep in mind however that these result in more false positives than positives.

- The first method is only effective in detecting users of NetStumbler. The second method can be used to detect users of NetStumbler, MiniStumbler, and MacStumbler.

- Since Kismet is a passive scanner, these methods cannot be used to detect users of that program.

- Both of these methods involve setting up a stationary computer with a wireless LAN card and running Kismet 24 hours a day.

- The computer will not be attached to the wireless network; it will simply be in passive "listen mode."

- Listening for NetStumbler signatures

  - The Kismet scanning application now has the ability to detect nearby wardrivers that are using NetStumbler.

  - A unique signature of NetStumbler is that it emits a packet of data after it has detected a wireless network.

  - This packet has a signature that can now be identified by Kismet.

- Listening for excessive 802.11b probe requests

  - A less accurate method of detecting wardrivers is to simply listen for an excess amount of 802.11b probe requests.

  - This will not positively identify all wardrivers because even legitimate 802.11b clients emit 802.11b probe requests.

Wireless Network Sniffing

- Once the reconnaissance activity has provided possible targets the next step is to passively sniff or eavesdrop on the network.

- Sniffing has long been a reconnaissance technique used in wired networks. Attackers sniff the frames necessary to enable the exploits that will be used in the active attacks used to compromise networks.

- Sniffing can also help find the easy target as in scanning for open APs that allow anyone to connect, or capturing the passwords used in a connection session that does not even use WEP.

- Detecting the presence of a wireless sniffer, who remains radio-silent, through network security measures is virtually impossible.

- Once the attacker begins probing (i.e., by injecting packets), the presence and the coordinates of the wireless device can be detected.

Passive Scanning

- Scanning is the act of sniffing by locking on to various radio channels and listening to the network traffic.

- A **passive** network scanner instructs the wireless card to listen to each channel for a few messages. This activity does not reveal the presence of the scanner.

- There is a mode called **RF monitor mode** that allows every frame appearing on a wireless channel to be copied as the receiver locks on to various channels.

- This is analogous to placing a wired Ethernet card in promiscuous mode. This mode is not enabled by default.

- The key to monitor mode is that a station in monitor mode can capture packets **without associating** with an AP or ad-hoc network.

- One of the oldest sniffers available is **Kismet** (http://www.kismetwireless.net).

- More current ones include **aircrack-ng** and **airodump-ng.**

Detection of the SSID

- The attacker can discover the SSID of a network usually by passive scanning because the SSID is available with the following frame types: Beacon, Probe Requests, Probe Responses, Association Requests, and Reassociation Requests.
- Recall that management frames are always in the clear, even when WEP is enabled. On a number of APs, it is possible to configure so that the SSID transmitted in the Beacon frames is masked, or even turn off Beacons altogether.
- The SSID shown in the Beacon frames is set to null in the hope of making the WLAN invisible unless a client already knows the correct SSID.
- In such a case, a station wishing to join a WiLAN begins the association process by sending Probe Requests since it could not detect any APs via Beacons that match its SSID.
- If the Beacons are not turned off, and the SSID in them is not set to null, an attacker obtains the SSID included in the Beacon frame by passive scanning.
- When the Beacon displays a null SSID, there are two possibilities. Eventually, an Associate Request may appear from a legitimate station that already has a correct SSID.
- To such a request, there will be an Associate Response frame from the AP. Both frames will contain the SSID in the clear, and the attacker sniffs these.
- If the station wishes to join any available AP, it sends Probe Requests on all channels, and listens for Probe Responses that contain the SSIDs of the APs.
- The station considers all Probe Responses, just as it would have with the non-empty SSID Beacon frames, to select an AP. Normal association then begins. The attacker waits to sniff these Probe Responses and extract the SSIDs.
- If Beacon transmission is disabled, the attacker can keep sniffing waiting for a voluntary Associate Request to appear from a legitimate station that already has a correct SSID and sniff the SSID as described above.
- The attacker can also chose to actively probe by injecting frames that he constructs, and then sniffs the response.
- If both the above methods fail, SSID discovery is done by **active** scanning.

Collecting the MAC Addresses

- The attacker gathers legitimate MAC addresses for use later in constructing spoofed frames.

- The source and destination MAC addresses are always in the clear in all the frames.

- There are two reasons why an attacker would collect MAC addresses of stations and APs participating in a wireless network:

- The attacker wishes to use these values in spoofed frames so that his station or AP is not identified.

- The targeted AP may be controlling access by filtering out frames with MAC addresses that were not registered.

Collecting the Frames for Cracking WEP

- Once a large number of frames have been sniffed from a closed network, an attacker will attempt to discover the WEP shared-secret key.

- Often, the shared key can be discovered by guesswork based on a certain amount of social engineering regarding the administrator who configures the wireless LAN and all its users.

- Some client software stores the WEP keys in the operating system registry or initialization scripts.

- The attacker will use automated software application to process the WEP encrypted frames.

- For this purpose, a large number (millions) of frames need to be collected because of the way WEP works.

- Certain cards are so simplistic that they start their Initialization Vector (IV) as 0 and increment it by 1 for each frame, resetting in between for some events.

- Even the better cards generate weak IVs from which the first few bytes of the shared key can be computed after statistical analyses.

- Some implementations generate fewer mathematically weak vectors than others do. The attacker sniffs a large number of frames from a single BSS. These frames all use the same key.

- What is needed however is a collection of frames that were encrypted using “mathematically-weak” IVs.

- The number of encrypted frames that were mathematically weak is a small percentage of all frames.

- In a collection of a million frames, there may only be a hundred mathematically weak frames. It is conceivable that the collection may take a few hours to several days depending on how busy the WiLAN is.

- Given a sufficient number of mathematically weak frames, the systematic computation that exposes the bytes of the secret key is intensive.

- However, an attacker can employ powerful computers. On an average PC, this may take a few seconds to hours. The storage of the large numbers of frames is in the several hundred-mega bytes to a few Gigabytes range.

- One of the best WEP cracking tools available is AirSnort (http://airsnort.shmoo.com).

Wireless Spoofing

- There are well-known attack techniques known as spoofing in both wired and wireless networks.

- The attacker constructs frames by filling selected fields that contain addresses or identifiers with legitimate looking but non-existent values, or with values that belong to others.

- The attacker would have collected these legitimate values through sniffing.

MAC Address Spoofing

- Skilled attackers will not want to reveal their presence. But the probing activity injects frames that are observable by system administrators.

- The attacker fills the **Sender MAC Address** field of the **injected frames** with a **spoofed value** so that the attacking equipment is not identified.

- Typical APs control access by permitting only those stations with known MAC addresses.

- Either the attacker has to compromise a computer system that has a station, or spoof with legitimate MAC addresses in frames that have been crafted.

- MAC addresses are assigned at the time of manufacture, but setting the MAC address of a wireless card or AP to an arbitrary chosen value is a simple matter of invoking an appropriate software tool that engages in a dialog with the user and accepts values.

- Such tools are routinely included when a station or AP is purchased. The attacker, however, changes the MAC address programmatically, sends several frames with that address, and repeats this with another MAC address.

- In a period of a second, this can happen several thousand times.
- When an AP is not filtering MAC addresses, there is no need for the attacker to use legitimate MAC addresses.

- However, in certain attacks, the attacker needs to have a large number of MAC addresses than can be collected by sniffing.

- Random MAC addresses are generated. However, not every random sequence of six bytes is a MAC address. The IEEE assigns globally the first three bytes, and the manufacturer chooses the last three bytes.

- The officially assigned numbers are publicly available. The attacker generates a random MAC address by selecting an IEEE-assigned three bytes appended with an additional three random bytes.

IP spoofing

- Replacing the true IP address of the sender (or, in rare cases, the destination) with a different address is known as IP spoofing; a necessary operation in many attacks.

- The IP layer simply trusts that the source address, as it appears in an IP packet is valid. It assumes that the packet it received indeed was sent by the host officially assigned that source address.

- Because the IP layer adds these IP addresses to a data packet when the header is created, a spoofing attack must circumvent the IP layer and communicate directly to the raw network device.

- IP spoofing is an integral part of many attacks. For example, an attacker can silence a host A from sending further packets to B by sending a spoofed packet announcing a window size of zero to A as though it originated from B.

Frame Spoofing

- The attacker will inject frames that are valid by 802.11 specifications, but whose content is carefully spoofed as described above.

- Frames themselves are not authenticated in 802.11 networks. So when a frame has a spoofed source address, it cannot be detected unless the address is completely bogus.

- If the frame to be spoofed is a management or control frame, there is no encryption to deal with. If it is a data frame, perhaps as part of an on-going MITM attack, the data payload must be properly encrypted.

- Construction of the byte stream that constitutes a spoofed frame is a programming matter once the attacker has gathered the needed information through sniffing and probing.

- There are software libraries that make this task relatively easy. Examples of such libraries are **libpcap** (sourceforge.net/projects/libpcap/), **libnet** (libnet.sourceforge.net/), **libdnet** (libdnet. sourceforge.net/) and **libradiate** (www.packetfactory.net/projects/libradiate/).

- The difficulty here is not in the construction of the contents of the frame, but in getting, it transmitted by the station or an AP.

- This requires control over the firmware and driver of the wireless card that may sanitize certain fields of a frame.

- Therefore, the attacker will select the spoofing equipment carefully. Currently, there are off-the-shelf wireless cards that can be manipulated to conduct spoofing attacks.

- In addition, the construction of special purpose wireless cards is within the reach of a resourceful attacker.

Wireless Network Probing

- An attacker can gather a considerable amount of information regarding a wireless network through sniffing, without revealing the presence of the sniffing equipment at all.

- However, there still may be missing pieces of information that would be required to run an exploit.

- If this is the case, an attacker can send a carefully crafted packet to a target in order to elicit useful responses.

- This activity is known as probing or active scanning. The target may discover that it is being probed.

Detection of the SSID

- Detection of SSID is often possible by simply sniffing Beacon frames as described earlier.

- If Beacon transmission is disabled, and the attacker does not wish to patiently wait for a voluntary Associate Request to appear from a legitimate station that already has a correct SSID, or Probe Requests from legitimate stations, he will inject a Probe Request frame that contains a spoofed source MAC address.

- The Probe Response frame from the APs will contain, in the clear, the SSID and other information similar to that in the Beacon frames were they enabled.

- The attacker sniffs these Probe Responses and extracts the SSIDs.

- Some models of APs have an option to disable responding to Probe Requests that do not contain the correct SSID.

- In this case, the attacker determines a station associated with the AP, and sends the station a forged Disassociation frame where the source MAC address is set to that of the AP.

- The station will send a Reassociation Request that exposes the SSID.

- As mention earlier, it is possible to detect the presence of probing activity.

- The frames that an attacker injects can also be heard by the intrusion detection systems (IDS) of a wireless LAN.

- There is GPS-enabled equipment that can identify the physical coordinates of a wireless device through which the probe frames are being transmitted.

AP Weaknesses

- APs have weaknesses that are both due to design flaws and user interfaces that promote weak passwords, etc.

- It has been demonstrated by many publicly conducted war-driving efforts (www.worldwidewardrive.org) in major cities around the world that a large majority of the deployed APs are poorly configured, most with WEP disabled, and configuration defaults, as set up the manufacturer, untouched.

Defeating MAC Filtering

- Typical APs permit access to only those stations with known MAC addresses.

- This can easily be defeated by the attacker who spoofs transmitted frames with a MAC address that is registered with the AP from among the ones that have been collected through sniffing.

- It can be verified that a MAC address is registered by observing the frames from the AP to the stations.

Rogue AP

- Access points that are deployed without proper authorization and verification that overall security policy is obeyed are called **rogue** APs.

- These are usually installed and used by valid users within an organization. Such APs are usually poorly configured, and are quickly identified by attackers and compromised.

Trojan AP

- An attacker sets up an AP so that the targeted station receives a stronger signal from the attacker's AP than what it receives from a legitimate AP.

- If WEP is enabled, the attacker would have already cracked it.

- A legitimate user selects the Trojan AP because of the stronger signal, authenticates and associates.

- The Trojan AP is connected to a system that collects the IP traffic for later analysis. It then transmits all the frames to a legitimate AP so that the victim user does not recognize the on-going MITM attack.

- The attacker can steal authentication information such as usernames and passwords, and then compromise the user's system to acquire root access.

- This attack is called the **Evil Twin Attack**. It is easy to build a Trojan AP because an AP is a computer system optimized for its intended application.

- A general purpose PC with a wireless card can be turned into a capable AP. An example of such software is **HostAP** (http://hostap.epitest.fi/).

Equipment Flaws

- There numerous flaws in equipment from well-known manufacturers that are well-known and exploited.

- For example, one such AP crashes when a frame is sent to it that has the spoofed source MAC address of itself.

- Another AP features an embedded TFTP (Trivial File Transfer Protocol) server. By requesting a file named config.img via TFTP, an attacker receives the binary image of the AP configuration.

- The image includes the administrator's password required by the HTTP user interface, the WEP encryption keys, MAC address, and SSID.

- Yet another AP returns the WEP keys, MAC filter list, administrator's password when sent a UDP packet to port 27155 containing the string "gstsearch".

- Most manufacturers design their equipment so that its firmware can be flashed with a new and improved one in the field.

- The firmware images are downloaded from the manufacturers' web site. The CPU used in the APs can be easily recognized, and the firmware can be systematically disassembled revealing the flaws at the assembly language level.

Denial of Service

- A **denial of service** (**DoS**) occurs when a system is prevented from providing services to authorized clients as a result of an attack that exhausts all of the available resources.

- In wireless networks, DoS attacks are difficult to prevent, difficult to stop an on-going attack and the victim and its clients may not even detect the attacks.

Jamming the Radio Channel

- A number of consumer appliances such as microwave ovens, baby monitors, and cordless phones operate on the unregulated 2.4GHz radio frequency.

- Generating and interfering signal in 802.11 networks is fairly simple. For example, a Bluetooth device is one such item when located within approximately 10m of an 802.1 device, generates a strong jamming signal.

- An attacker can generate a large amount of noise using other such devices and jam the channel so that the signal-to-noise ratio drops to a point where the wireless LAN ceases to function.

- The only solution to this is deploying RF shielding in the surrounding environment, i.e., at the perimeter.

Flooding with Associations

- The AP inserts the data supplied by the station in the Association Request into a table called the **association table** that the AP maintains in its memory.

- The 802.11 standard specifies a maximum value of 2007 concurrent associations to an AP. The actual size of this table varies among different models of APs.

- When this table overflows, the AP would refuse further clients.

- Having cracked WEP, an attacker authenticates several non-existing stations using legitimate-looking but randomly generated MAC addresses.

- The attacker then sends a flood of spoofed associate requests so that the association table overflows.

- Enabling MAC filtering in the AP will prevent this attack.

Forged Dissociation

- The attacker sends a spoofed Disassociation frame where the source MAC address is set to that of the AP.

- The station is still authenticated but needs only to Reassociate and sends Reassociation Requests to the AP.

- The AP may send a Reassociation Response accepting the station and the station can then resume sending data.

- To prevent Reassociation, the attacker continues to send Disassociation frames for a desired period.

Forged Deauthentication

- The attacker monitors all raw frames collecting the source and destination MAC addresses to verify that they are among the targeted victims.

- When a data or Association Response frame is observed, the attacker sends a spoofed Deauthentication frame where the source MAC address is spoofed to that of the AP.

- The station is now unassociated and unauthenticated, and needs to reconnect. To prevent a reconnection, the attacker continues to send Deauthentication frames for a desired period.

- The attacker may even rate limit the Deauthentication frames to avoid overloading an already congested network.

- These mischievous Disassociation and Deauthentication frames are sent directly to the client, so they will not be logged by the AP or IDS, and neither MAC filtering nor WEP protection will prevent it.

Power Saving

- Power conservation is important for typical station laptops, so they frequently enter an 802.11 state called Doze.

- An attacker can steal packets intended for a station while the station is in the Doze state.

- The 802.11 protocol requires a station to inform the AP through a successful frame exchange that it wishes to enter the Doze state from the Active state.

- Periodically the station awakens and sends a PS-Poll frame to the AP. The AP will transmit in response the packets that were buffered for the station while it was dozing.
- This polling frame can be spoofed by an attacker causing the AP to send the collected packets and flush its internal buffers.

- An attacker can repeat these polling messages so that when the legitimate station periodically awakens and polls, AP will inform that there are no pending packets.

Man-in-the-Middle Attacks

- Man-in-the-middle (**MITM**) attack refers to the situation where an attacker on host X inserts X between all communications between hosts B and C, and neither B nor C is aware of the presence of X.

- All messages sent by B do reach C but via X, and vice versa. The attacker can merely observe the communication or modify it before sending it out.

- An MITM attack can break connections that are otherwise secure. At the TCP level, SSH and VPN, e.g., are prone to this attack.

Wireless MITM

- Assume that station B was authenticated with C, a legitimate AP. Attacker X is a laptop with two wireless cards.

- Through one card, he will present X as an AP. Attacker X sends Deauthentication frames to B using the C's MAC address as the source, and the BSSID he has collected.

- B gets deauthenticated and begins a scan for an AP and may find X on a channel different from C.

- There is a race condition between X and C. If B associates with X, the MITM attack succeeded.

- X will re-transmit the frames it receives from B to C, and the frames it receives from C to B after suitable modifications.

- The package of tools called AirJack (http://802.11ninja.net/airjack/) includes a program called monkey_jack that automates the MITM attack.

- This is programmed well so that the odds of it winning in the race condition mentioned above are improved.

ARP Poisoning

- ARP cache poisoning is an old and tested exploit in wired networks. Wired networks have deployed mitigating techniques.

- But, the ARP poisoning technique is re-enabled in the presence of APs that are connected to a switch/hub along with other wired clients.

- Unfortunately, the ARP protocol does not provide for any verification that the responses are from valid hosts or that it is receiving a gratuitous ARP response as if it had sent an ARP Request.

- ARP poisoning is an attack technique exploiting this lack of verification. It corrupts the ARP cache in that the system associates an invalid MAC addresses for one of the IP addresses under its control.

- An attacker accomplishes this by sending an ARP Reply packet that is deliberately constructed with a “wrong” MAC address.

- Keeping in mind that ARP is a stateless protocol, a machine receiving an ARP Reply cannot determine if the response is due to a request it sent or not.

- ARP poisoning is one of the techniques that enables the man-in-the-middle attack. An attacker on machine X inserts himself between two hosts B and C by:

    - poisoning B so that C's IP address is associated with X's MAC address,
    - poisoning C so that B's address is associated with X's MAC address, and
    - relaying the packets X receives.

- The ARP poison attack is applicable to all hosts in a subnet. Most APs act as transparent MAC layer bridges, and so all stations associated with it are vulnerable.

- If an access point is connected directly to a hub or a switch without an intervening router/firewall, then all hosts connected to that hub or switch are susceptible also.

- Note that devices aimed at the home consumer market combine a network switch with four or five ports, an AP, a router and a DSL/cable modem connecting to the Internet at large.

- Internally, the AP is connected to the switch. As a result, an attacker on a wireless station can become a MITM between two wired hosts, one wired one wireless, or both wireless hosts.

- The tool called Ettercap ((http://ettercap.sourceforge.net) is capable of performing ARP poisoning.

- Another such tool is called Dsniff (http://www.monkey.org/~dugsong/dsniff/).

Session Hijacking

- Session hijacking occurs in the context of a "user", whether human or computer. The user has an on-going connection with a server.

- Hijacking is said to occur when an attacker causes the user to lose his connection, and the attacker assumes that user's identity and privileges for a period of time.

- An attacker disables temporarily the user's system, say by a DoS attack or a buffer overflow exploit.

- The attacker then takes the identity of the user. The attacker now has all the access that the user has.

- The user is allowed to resume once the DoS attack is stopped. The user may not detect the interruption if the disruption lasts no more than a couple of seconds.

- Such hijacking can be achieved by using forged Disassociation DoS attack.

- Corporate wireless networks are often set up so that the user is directed to an authentication server when a station attempts a connection with an AP.

- After the authentication, the attacker employs the session hijacking described above using spoofed MAC addresses.