Unit 5

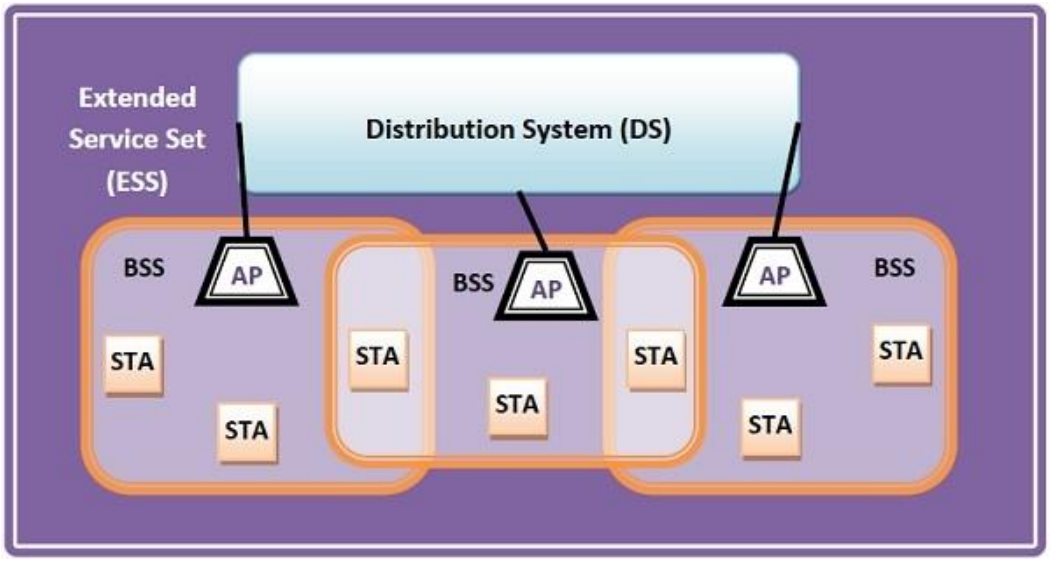
Wireless Security: IEEE 802.11

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows −

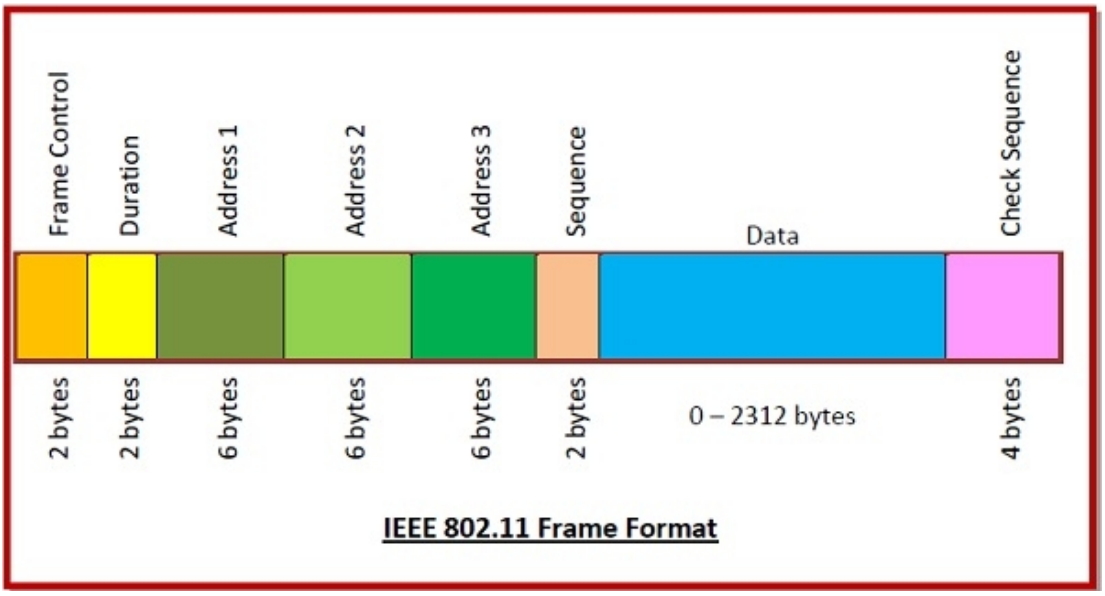
- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
    - Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
    - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.
- Each station has a wireless network interface controller.
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation−
    - Infrastructure BSS − Here, the devices communicate with other devices through access points.
    - Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.



Frame Format of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
- **Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.
- **Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.



Wireless LAN security :-

Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include the following

• Channel: Eavesdropping and jamming than wired networks. Wireless networks are also more vulnerable to active attacks that exploit

• Mobility: Mobility results in a number of risks.

• Resources: Limited memory and processing resources with which to counter threats, including denial of service and malware.

• Accessibility: Greatly increases their vulnerability to physical attacks.

Wireless Network Threats (1

• Accidental association : A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network.

• Malicious association : a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.

• Ad hoc networks : peer-to-peer networks between wireless computers with no access point between them

• Nontraditional networks : Nontraditional networks and links, such as personal network Bluetooth devices, barcode readers, and handheld PDAs, pose a security risk in terms of both eavesdropping and spoofing.

Wireless Network Threats (2)

• Identity theft (MAC spoofing): This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.

• Man-in-the middle attacks: This attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device. Wireless networks are particularly vulnerable to such attacks.

• Denial of service (DoS): The wireless environment lends itself to this type of attack, because it is so easy for the attacker to direct multiple wireless messages at the target.

• Network injection: A network injection attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages. An example of such an attack is one in which bogus reconfiguration commands are used to affect routers and switches to degrade network performance.

Wireless Security Measures (1)

Securing Wireless Transmissions principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption

• **Signal-hiding techniques**: Organizations can take a number of measures to make it more difficult for an attacker to locate their wireless access points, including turning off service set identifier (SSID) broadcasting by wireless access points; assigning cryptic names to SSIDs; reducing signal strength to the lowest level that still provides requisite coverage; and locating wireless access points in the interior of the building, away from windows and exterior walls. Greater security can be achieved by the use of directional antennas and of signal-shielding techniques.

• **Encryption**: Encryption of all wireless transmission is effective against eavesdropping to the extent that the encryption keys are secured.

Wireless Security Measures (2 Securing Wireless Access Points The main threat involving wireless access points is unauthorized access to the network. The principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control. Securing Wireless Networks

1. Use encryption. Wireless routers are typically equipped with built-in encryption mechanisms for router-to-router traffic.
2. Use antivirus and antispyware software, and a firewall.
3. Turn off identifier broadcasting. If a network is configured so that authorized devices know the identity of routers, this capability can be disabled, so as to thwart attackers.
4. Change the identifier on your router from the default.
5. Change your router's pre-set password for administration. This is another prudent step.
6. Allow only specific computers to access your wireless network. A router can be configured to only communicate with approved MAC addresses.

Authentication in wireless lan

802.11 authentication is the first step in network attachment. 802.11 authentication requires a mobile device (station) to establish its identity with an Access Point (AP) or broadband wireless router. No data encryption or security is available at this stage.

The Institute of Electrical and Electronics Engineers, Inc.(IEEE) 802.11 standard defines two link-level types of authentication:

- Open System
- Shared Key

Open system authentication

Open system authentication consists of two communications:

1. First, an authentication request is sent from the mobile device that contains the station ID (typically the MAC address).
2. Next, an authentication response from the AP/router with a success or failure message.

Shared key authentication

With shared key authentication, a shared key, or passphrase, is manually set on both the mobile device and the AP/router. Several types of shared key authentication are available today for home or small office WLAN environments:

Authentication and confidentiality Wireless security confidentiality attack :-

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 (at least for today) 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 authentication attack

authentication is the method of verifying the presented identity and credentials. Most of the authentication schemes used in wireless setups are secured with proper encryption.

We have already described the scenario based on EAP-authentication used in WPA/WPA2, with PSK authentication. By sniffing the 4-way handshake between the client and the authenticator (AP), one may perform a brute-force attack (example – offline dictionary attack) to break the encryption and derive the PSK value.

Another example can be LEAP (Lightweight Extensible Authentication Protocol). It was used in olden times as a mechanism to generate dynamic WEP keys. In this setup, the password hashes were flowing over-the-air hashed with MS-CHAP or MS-CHAPv2 algorithms (both of them are crack-able with an offline dictionary attack). A short description of the authentication attack that may be applied to LEAP would consist of the following steps −

- The username is sent in a clear text.
- There is a challenge text in clear text.
- The response text is hashed.
- Office dictionary attack, that can be used here (using **aircrack-ng** tool) to try all the combinations of the password inside "**function(password,challenge)** = **response**" mathematical formula, to find the right password.

Cellphone Security

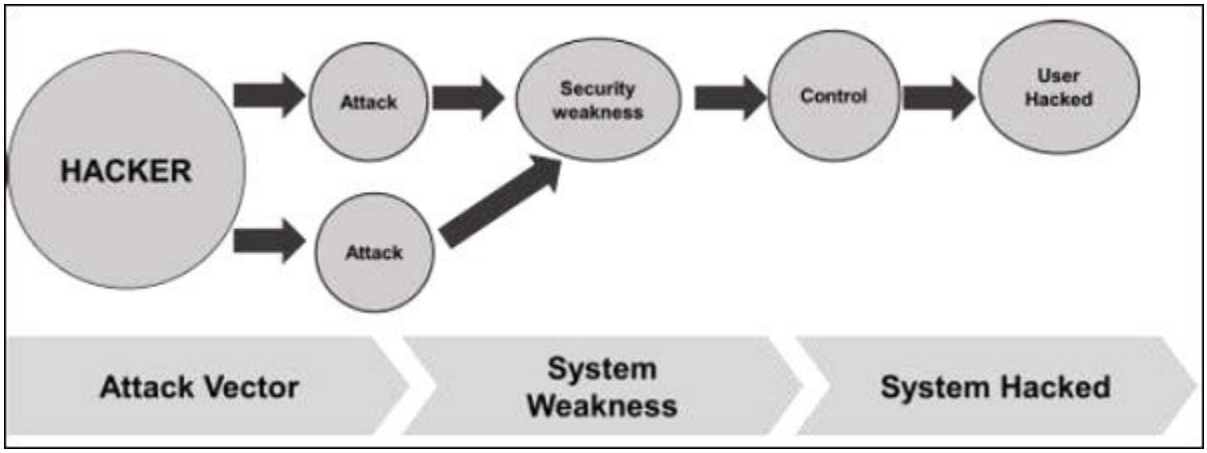
Mobile Security as a concept deals with the protection of our mobile devices from possible attacks by other mobile devices, or the wireless environment that the device is connected to.

Following are the major threats regarding mobile security −

- Loss of mobile device. This is a common issue that can put at risk not only you but even your contacts by possible phishing.
- Application hacking or breaching. This is the second most important issue. Many of us have downloaded and installed phone applications. Some of them request extra access or privileges such as access to your location, contact, browsing history for marketing purposes, but on the other hand, the site provides access to other contacts too. Other factors of concern are Trojans, viruses, etc.
- Smartphone theft is a common problem for owners of highly coveted smartphones such as iPhone or Android devices. The danger of corporate data, such as account credentials and access to email falling into the hands of a tech thief is a threat.

Mobile Security - Attack Vectors

By definition, an **Attack Vector** is a method or technique that a hacker uses to gain access to another computing device or network in order to inject a “bad code” often called **payload**. This vector helps hackers to exploit system vulnerabilities. Many of these attack vectors take advantage of the human element as it is the weakest point of this system. Following is the schematic representation of the attack vectors process which can be many at the same time used by a hacker.



Some of the mobile attack vectors are −

- Malware
  - Virus and Rootkit
  - Application modification
  - OS modification
- Data Exfiltration
  - Data leaves the organization
  - Print screen

- Copy to USB and backup loss

- Data Tampering
  - Modification by another application
  - Undetected tamper attempts
  - Jail-broken devices

- Data Loss
  - Device loss
  - Unauthorized device access
  - Application vulnerabilities

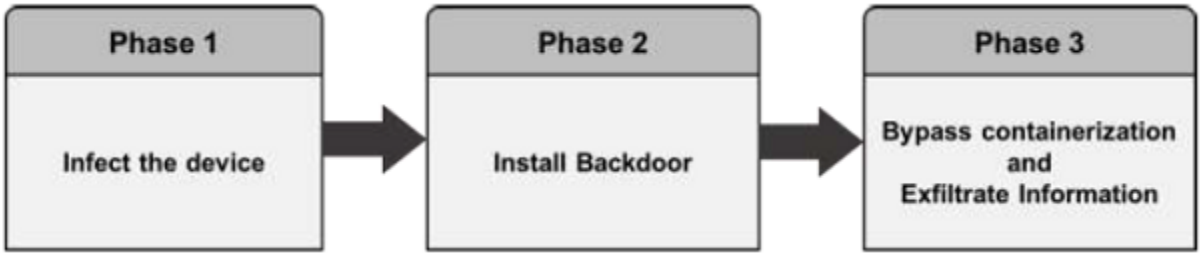
Consequences of Attack Vectors

Attack vectors is the hacking process as explained and it is successful, following is the impact on your mobile devices.

- **Losing your data** − If your mobile device has been hacked, or a virus introduced, then all your stored data is lost and taken by the attacker.
- **Bad use of your mobile resources** − Which means that your network or mobile device can go in overload so you are unable to access your genuine services. In worse scenarios, to be used by the hacker to attach another machine or network.
- **Reputation loss** − In case your Facebook account or business email account is hacked, the hacker can send fake messages to your friends, business partners and other contacts. This might damage your reputation.
- **Identity theft** − There can be a case of identity theft such as photo, name, address, credit card, etc. and the same can be used for a crime.

Anatomy of a Mobile Attack

Following is a schematic representation of the anatomy of a mobile attack. It starts with the infection phase which includes attack vectors.



Infecting the device

Infecting the device with mobile spyware is performed differently for Android and iOS devices.

Android − Users are tricked to download an app from the market or from a third-party application generally by using social engineering attack. Remote infection can also be performed through a Man-in-the-Middle (MitM) attack, where an active adversary intercepts the user's mobile communications to inject the malware.

iOS − iOS infection requires physical access to the mobile. Infecting the device can also be through exploiting a zero-day such as the JailbreakME exploit.

Installing a backdoor

To install a backdoor requires administrator privileges by rooting Android devices and jailbreaking Apple devices. Despite device manufacturers placing rooting/jailbreaking detection mechanisms, mobile spyware easily bypasses them −

Android − Rooting detection mechanisms do not apply to intentional rooting.

iOS − The jailbreaking "community" is vociferous and motivated.

Bypassing encryption mechanisms and exfiltrating information

Spyware sends mobile content such as encrypted emails and messages to the attacker servers in plain text. The spyware does not directly attack the secure container. It grabs the data at the point where the user pulls up data from the secure container in order to read it. At that stage, when the content is decrypted for the user's usage, the spyware takes controls of the content and sends it on.

GSM (2G) Security :-

The first GSM networks started appearing around the world in the early 1990's and their adoption by the general public grew at an ever faster pace. By the dusk of the last millennium around 50% of the adult population in the developed world owned a mobile phone. The trend continued moving linearly in the up directions until almost reaching 100% by the end of the last decade. Mobile phones had become truly ubiquitous and many people wondered how one could live a normal life before the ascent of mobile technologies. Mobile Station Authentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.

The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.

The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

Signalling and Data Confidentiality

The SIM contains the ciphering key generating algorithm (A8) that is used to produce the 64-bit ciphering key (Kc). This key is computed by applying the same random number (RAND) used in the authentication process to ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).

GSM provides an additional level of security by having a way to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required. As in case of the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore, sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.

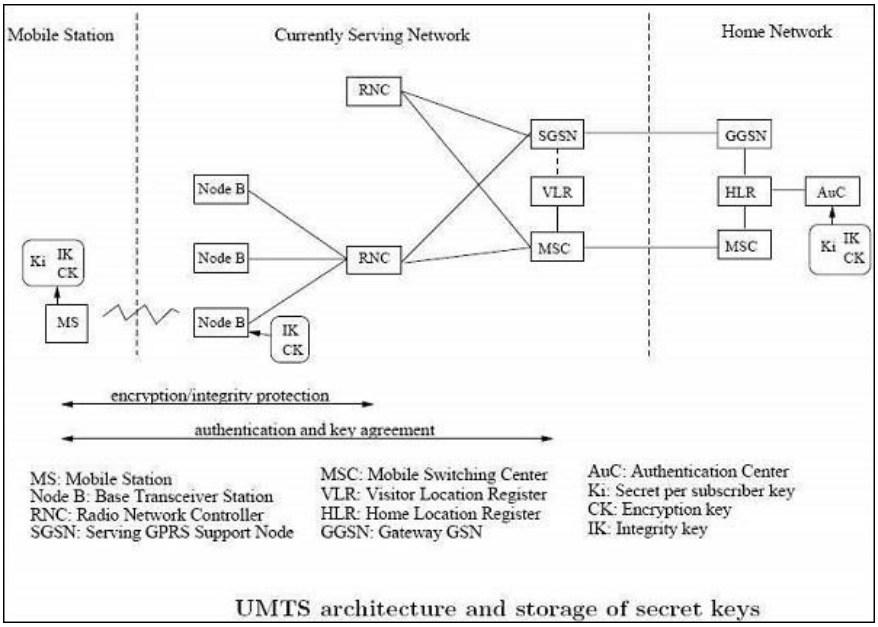
Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).

Subscriber Identity Confidentiality

To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station. After the receipt, the mobile station responds. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.

Security in UMTS (3G)

UMTS is designed to interoperate with GSM networks. To protect GSM networks against man-in-middle attacks, 3GPP is considering to add a structure RAND authentication challenge.

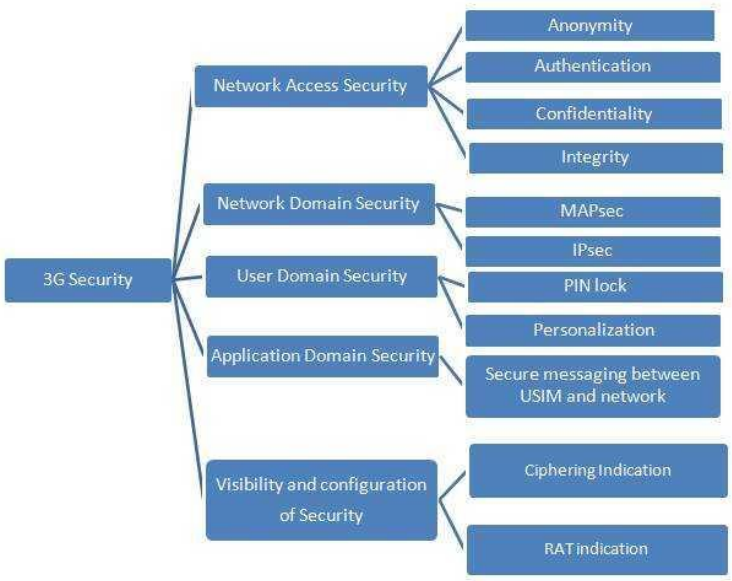


UMTS architecture and storage of secret keys

In UMTS, security mechanism is developed to take care of all the gsm security shortfalls. UMTS security is also referred as 3G security.

Five security groups exist in 3G networks as shown in the figure.

- Network Access Security
- Network domain security
- User domain security
- Application domain security
- visibility, configurability of security



Network Access Security helps protect air interface and also provide 3g subscribers to access the 3g network securely. In UMTS authentication, key 'K' is shared between network and UE. The network transmits random generated number 'RAND' and 'AUTN' in the message authentication challenge to the UE. AUTN makes it possible for UE to authenticate the 3g network. USIM generates response back to the network with ciphering and integrity keys. This helps network authenticate the UE.

The major difference between gsm security and **3g security** is that network authentication was not possible with gsm compliant UE. This is possible in UMTS compliant UE.

cipher key (Kc) in 3g security is of length 128 bits which was 64 bits in gsm. In gsm, ciphering was provided to air interface only and ciphering between MS and BTS is not provided. In UMTS, security is provided between UTRAN and RNC. Hence 3g security is extended between UE and RNC.

Wireless LAN Vulnerabilities

Below are seven of the most common threats to wireless networks.

- Configuration Problems (Misconfigurations or Incomplete Configurations) ...
- Denial of Service. ...

- Passive Capturing. ...
- Rogue (or Unauthorized/Ad-Hoc) Access Points. ...
- Evil Twin Attacks. ...
- Hacking of Lost or Stolen Wireless Devices. ...
- Freeloading.

Network Threats (and How to Protect Against Them)

While deceitful actions do commonly occur, there are also many accounts of innocent, yet careless, actions are often the cause of a major security breach. Below are seven of the most common threats to wireless networks.

1. Configuration Problems (Misconfigurations or Incomplete Configurations)

Simple configuration problems are often the cause of many vulnerabilities because many consumer/SOHO-grade access points ship with no security configuration at all. Other potential issues with configuration include weak passphrases, feeble security deployments, and default SSID usage.

A novice user can quickly set up one of these devices and gain access, or open up a network to external use without further configuration. These acts allow attackers to steal an SSID and connect without anyone being the wiser.

To mitigate the risk, use a centrally managed WLAN that features periodic audits and coordinated updates.

2. Denial of Service

Anybody familiar with network security is aware of the concept of denial of service (DoS), also referred to as a “spoiler.” It is one of the simplest network attacks to perpetrate because it only requires limiting access to services. This can be done by placing viruses or worm programs on your network, or by simply sending a large amount of traffic at a specific target with the intent of causing a slowdown or shutdown of wireless services. This allows attackers to hijack resources, view unauthorized information disclosures, and introduce backdoors into the system.

For wireless networks it can be much easier, as the signal can be interfered with through a number of different techniques. When a wireless LAN is using the 2.4 GHz band, interference can be caused by something as simple as a microwave oven or a competing access point on the same channel. Because the 2.4 GHz band is limited to only three non-overlapping channels (in the U.S.), an attacker just needs to cause enough interference into these to cause service interruption.

A denial of service attack can also be used in conjunction with a rogue access point. For example, one could be set up in a channel not used by the legitimate access point. Then a denial of service attack could be launched at the channel currently being used, causing endpoint devices to try and re-associate onto a different channel that is used by the rogue access point.

3. Passive Capturing

Passive capturing (or eavesdropping) is performed simply by getting within range of a target wireless LAN, then ‘listening to’ and capturing data which can be used for breaking existing security settings and analyzing non-secured traffic. Such information that can be “heard” include SSIDs, packet exchanges, and files (including confidential ones).

Consider the following scenarios that make passive capturing possible:

- Your office building has multiple tenants, including immediately above or below you on different floors.
- You have a lobby just outside your office.
- Your parking lot is close to the building.
- There is a street that passes nearby.
- There are adjacent buildings.

When it comes down to it, passive capturing is possible nearly anywhere. There are also some go-arounds when an attacker can't be within normal broadcast range, such as using a big antenna or a wireless repeater device to extend range by miles. An attacker can even use a packet sniffer application that captures all the outgoing packets, grabs and analyzes them, then reveals its data payload. You can try a packet sniffer yourself to see the depth and breadth of classified information that is available to anyone who wants to hijack it.

It is almost impossible to totally prevent this type of attack because of the nature of a wireless network. What can be done involves implementing high security standards by using a firewall, and setting complex parameters.

4. Rogue (or Unauthorized/Ad-Hoc) Access Points

One method often used by attackers involves setting up a rogue access point within the range of an existing wireless LAN. The idea is to 'fool' some of the authorized devices in the area to associate with the false access point, rather than the legitimate one.

To really be effective, this type of attack requires some amount of physical access. This is required because if a user associates with a rogue access point, then is unable to perform any of their normal duties, the vulnerability will be short-lived and not that effective. However, if an attacker is able to gain access to a physical port on a company network and then hook the access point into this port, it's possible to get devices to associate and capture data from them for an extended period of time.

The exception to this barrier is when the wireless LAN being targeted only provides internet access. A rogue access point can also offer simple internet access and leave the user unaware of their vulnerability for an extended amount of time.

Part of the same idea of rogue access points is unauthorized, non-malicious access points and ad-hoc networks. In these situations, a legitimate user sets up an access point or ad-hoc network for their own use, but does not implement proper security techniques. This provides an opening for watching attackers.

Some steps you can take to prevent such access points are to:

- Use proper WLAN authentication techniques and encryption methods.
- Establish and communicate a policy prohibiting employees from using their own wireless access points.

- Make it easier for employees to gain access to legitimate (and secured) wireless access points.
- Regularly walk around your office with a wireless-equipped device to search for rogue access points, looking in every network outlet.
- Install a WIPS (wireless intrusion prevention system) to scan radio spectrums, searching for access points with configuration errors.

5. Evil Twin Attacks

An attacker can gather enough information about a wireless access point to impersonate it with their own, stronger broadcast signal. This fools unsuspecting users into connecting with the evil twin signal and allows data to be read or sent over the internet.

Server authentication and penetration testing are the only tools that will aid in ending evil twin attacks.

6. Hacking of Lost or Stolen Wireless Devices

Often ignored because it seems so innocent, but if an employee loses a smartphone, laptop, etc., that is authorized to be connected to your network, it's very easy for the finder or thief to gain full access. All that's necessary is to get past the password, which is quite simple to do.

Make it a policy and practice to have employees immediately report a misplaced or stolen device so that it can be remotely locked, given a password change, or wiped clean.

7. Freeloading

Sometimes unauthorized users will piggyback on your wireless network to gain free access. Usually this is not done maliciously, but there are still security ramifications.

1. Your internet service may slow down.
2. Illegal content or spam can be downloaded via your mail server.
3. "Innocent" snooping may take place.

Additionally, employees sharing files with unrecognized networks, or giving permission for a friend or family member to use their login credentials for computer access, both seriously disrupt security measures.

Phishing:-

Phishing is a type of Social Engineering attack in which the victims are psychologically manipulated to provide sensitive information or install malicious programs. It is similar to 'fishing.' While in fishing, the fishermen use the fish food as the bait to trap fishes into fishing-net or fishing rod, in Phishing the cyber attackers use fake offers, warnings as bait to trap users into their scam.

The attackers can perform Phishing through emails, SMS, phone call, fake websites, and even face to face.

We will now discuss how Phishing is performed through different mediums.

How is Phishing Performed through Emails

For performing Phishing through emails, Cybercriminals follow these steps −

- At first, the targets are finalized, and details about them are collected. The target can be an individual, group of people or an organization.

- Now, the email message is framed based on the details gain from the previous step. For example, a fake banking email is prepared by knowing in which bank the target's account is. Similarly, Netflix users whose subscription is soon going to end, get fake subscription extension emails.

- In this step, the email is sent to the targets with a catchy subject line and pictures. The mail is sent to thousands of people so that at least hundreds of them can get into the trap.

- After getting a response from a few people, the Phisher now collects the sensitive information or makes them download and install the malicious programs.

- In the last step, the information obtained from the previous steps would be used to conduct illicit activities like stealing money from the bank, hacking social media sites, and more.

This is a generalized pattern an attacker follows in conducting Phishing through emails. There are various other ways too.

Buffer Overflow:-

A buffer overflow arises when a program tries to store more data in a temporary data storage area (buffer) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, thus corrupting the valid data held in them.

Example

Here is a classic examples of buffer overflow. It demonstrates a simple buffer overflow that is caused by the first scenario in which relies on external data to control its behavior. There is no way to limit the amount of data that user has entered and the behavior of the program depends on the how many characters the user has put inside.

Format String Attacks:-

How does format string attack work?

Format String attacks **alter the flow of an application**. They use string formatting library features to access other memory space. Vulnerabilities occurred when the user-supplied data is deployed directly as formatting string input for certain C/C++ functions (e.g., fprintf, printf, sprintf, setproctitle, syslog, ...).

SQL Injection:-

SQL injection is **a code injection technique that might destroy your database**. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.
What is SQL injection and how it works?

In SQL Injection, **the UNION operator is commonly used to attach a malicious SQL query to the original query intended to be run by the web application**. The result of the injected query will be joined with the result of the original query. This allows the attacker to obtain column values from other tables.

Virtual Elections:-