Hello Everyone! In this video, you will learn about wireless networks and various protocols used for securing them.

Wireless networks are computer networks, in which machines are not connected by cables of any kind. The wireless networks are based on radio waves, a transmission medium, without any cable. Wireless technologies are widely used in both home and business computer networks.

Based on Scale, wireless networks may be categorized as Personal area networks, local area networks, or metropolitan area networks.
A wireless personal area network allows the connectivity of personal devices within an area of about 10 meters. Bluetooth networks are an example.
Whereas, wireless local area networks allow users in a local area, typically within a range of 100 meters, such as a university campus or library, to form a network or gain access to the Internet. Wi-Fi networks which are also known by their standard name IEEE 802.11 are examples of wireless local area networks.

The third category of wireless networks is the metropolitan area network, which allows the connection of multiple networks in a metropolitan area such as different buildings in a city. It can be an alternative or backup to laying copper or fiber cabling. Wi-Max technology or wireless broadband service is an example of a wireless metropolitan area network.

Based on the availability of the Access point (the central point in a wireless network), the wireless networks can be either ad-hoc networks or Infrastructure networks.

In ad hoc networks, the computers act in a stand-alone way, communicating with each other in peer-to-peer communication mode. No access point (routers or switches) is required for communication between devices.

For setting up ad hoc mode, we need to manually configure the wireless adaptors of all devices to be in ad hoc mode., and all adaptors must use the same channel name or SSID for making the connection active.

The other architecture in a wireless network is centrally coordinated (infrastructure mode). All devices are connected to wireless network with the help of Access Point (AP). Wireless APs are usually routers or switches which are connected to the internet by broadband modem.

Infrastructure mode deployments are more suitable for larger organizations. The infrastructure mode provides improved security, ease of management, and much more scalability and stability. However, the infrastructure mode incurs extra cost in deploying access points such as routers or switches.

Using wireless networks offers many advantages.

They enable mobility while working, which is not possible with wired networks. This mobility results in flexibility of working space. The wireless nature of communication also allows expandability. Grow your network efficiently, adding new users and locations without needing to run cables and wires.

As the data in wireless networks moves through an open environment, an additional feature, encryption, is also provided, which is not available with other LAN standards commonly. Wireless encryption is the process of protecting a wireless network from attackers who attempt to collect sensitive information by breaching Radio Frequency traffic.

Wi-Fi networks initially used the encryption technique Wired equivalent privacy known as WEP in short. Over time the WEP technique was modified and later replaced with Wi-Fi protected Access(WPA) technique, which is now being used as WPA3 for the latest security arrangements in Wi-Fi networks. Let's discuss these techniques one by one.

WEP or Wired equivalent privacy was the first algorithm implemented for Wi-Fi networks. It used RC4 rivest cipher 4 for encryption with 64 and 128-bit keys and used 24 bits' keys as the initialization vector for encryption. This technique could provide privacy, authentication and data integrity.

WEP algorithm is not free from flaws. It has certain flaws, which make it less useful for securing wireless communication such as No defined method of distributing the keys is available. The keys, once set are rarely changed, which makes the recovery of messages in the long run possible, by the attackers.

Wi-Fi protected access or WPA is the improved algorithm that overcame the flaws of WEP. WPA used 256-bit keys for encryption and keys are renewed periodically.

But these features were not enough for protection from the attacks and WPA networks were also attacked like WEP. Therefore, WPA2 was introduced, which uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol(CCMP), better than the Temporal Key Integrity Protocol (TKIP) protocol used in WPA making it more difficult for attackers to break it. However, WPA2 was also breakable which lead to the introduction of WPA3.

The latest version of WPA, WPA3 has the following features. Secured handshake for making parties ready to communicate, Wi-Fi Easy Connect to simplify the security configuration process. It also helps set up a connection between different IoT devices. It uses a new feature called Opportunistic Wireless Encryption (OWE) that replaces the 802.11 “open” authentication by providing better protection when using public hotspots and public networks and uses bigger session keys to provide higher level of protection.

Thank You