# CLASS : T.E. (E&TC) SUBJECT: NETWORK SECURITY LAB

**EXPT. NO.: 07 DATE:**

**Title:** Study of different wireless network components and features of any one of the Mobile Security Apps. **Aim:** To study of different wireless network components and features of any one of the Mobile Security Apps.

# Student will be able to study mobile & web security

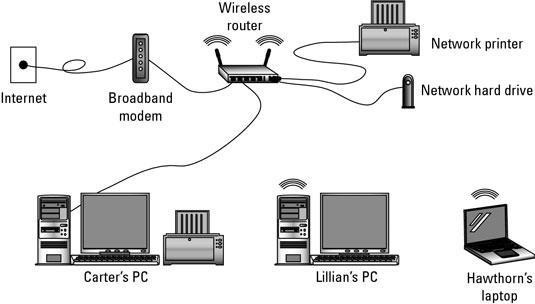
**Objectives:** After performing this experiment, the learner will be able to

1. Know about the devices and components in a wireless network.
2. Identify a mobile security app and how it works for mobile security?

# Component used: Computer with internet connectivity. Theory:

**Different wireless network components:**

As long as you have all the hardware, you can quickly set up any wireless network. Here is everything you need to know about the hardware you need to have in place before you use Windows to configure the wireless network. There are two types of wireless networks: infrastructure and ad hoc. The infrastructure network is most likely the type of wireless setup you have in your home or office. It’s laid out similarly to a wired network, but without wires.



# Figure: peer-to-peer network components

The basic wireless, peer-to-peer network consists of these components:

# Wireless Network Adapters:

Wireless network adapters (also known as wireless NICs or wireless network cards) are required for each device on a wireless network. All newer laptop computers incorporate wireless adapters as a built-in feature of the system.

No wireless hardware other than adapters is required to build a small local network. However, to increase the performance of network connections, accommodate more computers, and increase the network's range, additional types of hardware can be deployed.

# Wireless Routers:

Wireless routers function comparably to traditional routers for wired Ethernet networks. One generally deploys wireless routers when building an all-wireless network from the ground up.

Similar to routers, access points allow wireless networks to join an existing wired network. One typically deploys access points when growing a network that already has routers installed. In home networking, a single access point (or router) possesses sufficient range to span most residential buildings. Businesses in office buildings often must deploy multiple access points and/or routers.

# Wireless Antennas:

Access points and routers often utilize a Wi -Fi wireless antenna that significantly increase the communication range of the wireless radio signal. These antennas are optional and removable on most equipment. It's also possible to mount aftermarket add-on antennas on wireless clients to increase the range of wireless adapters. **Wireless Repeaters:**

A wireless repeater connects to a router or access point. Often called signal boosters or range expanders, repeaters serve as a two-way relay station for wireless radio signals, helping clients otherwise unable to receive a network's wireless signal to join.

Wire-based connections: Almost every wireless router has one or more standard, wire-based Ethernet port. One port is used to connect the router to a broadband modem. Other Ethernet ports might be also available, allowing you to connect standard wire-based networking to the wireless hub.

Wireless NIC: Your computer needs a wireless Network Interface Card, or NIC, to talk with the wireless router. A laptop comes standard with a wireless NIC, but for a desktop PC you have to get a wireless NIC as an option. It’s installed internally as an expansion card, or you can use one of the various plug-in USB wireless NICs.

These are the components for infrastructure type of wireless network. The other type of network called the ad hoc type of wireless network is basically a group of wireless computers connected with each other. An ad-hoc network has no central hub or router. Instead, all its computers can directly access the other computers’ files and shared resources. They may or may not have Internet access, but that’s not the point of the ad hoc network. One of the beauties of a wireless network is that you can mix in wired components as needed. If you need more Ethernet ports, for example, simply add a switch to the wireless router.

Despite the wireless nature of wireless networking, you still need an Ethernet cable (a wire) to connect a wireless router to a broadband modem.

Another advantage of a wireless network is that it’s portable. It’s far easier to pull up stakes with a wireless network than to pack up all the bits and pieces of a wired network. If you live in an apartment, or just move around a lot, wirelesses setup a good option.

The term access point is often abbreviated AP. Don’t be puzzled when you see the words wireless AP — it simply refers to the access point, not to the Associated Press.

A wireless network is often called a WLAN, for wireless local-area network.

A wireless network is also referred to by the term Wi-Fi. It stands for wireless fidelity.

Ad hoc networks are often used by computer gamers to gather in a single location to play games with each other.

# Mobile App Security

Mobile App security is the extent of protection that mobile device applications (apps)

Have from malware and the Activities of crackers and other criminals. The term can also refer to various technologies and production practices that minimize the risk of exploits to mobile devices through their apps.A mobile device has numerous components, all of them vulnerable to security weaknesses. The parts are made, distributed, and used by multiple players, each of whom plays a crucial role the security of a device. Each player should incorporate security measures into mobile devices as they are designed and built and into mobile apps as they are conceived and written, but these tasks are not always adequately carried out.

Common vulnerabilities for mobile devices include architectural flaws, device loss or theft, platform weakness, isolation and permission problems and application weaknesses. When evaluating mobile devices and apps for security, developers should ask themselves the following questions.

**How do users obtain a particular app? Should a firm create its own app store?**

How is an app vetted before it is offered for sale? How is an app protected against malware?

How can users tell the difference between a legitimate app and a fake? How easily can automatic update features get hijacked?

What measures exist to control the risk of device jail breaking? What kind of permissions should a particular app ask for?

Can any other apps keep track of when, where, and how a certain app is used?

Let us now discuss the features of a popular mobile security app called CM Security.

# CM Security

CM security (Clean Master) is an all-singing, all-dancing option made by Cheetah Mobile that brings you a whole host of anti-virus and security features for free - as long as you don't mind a few ads.

Features of CM security

Feature -wise it tries to offer everything - anti-virus, browsing protection, battery saving, privacy protection of apps, the whole lot. It takes pretty much the same simplified approach to each of those things too. CM security identifies what it describes as threats and then asks what you want to do about them in a straightforward way.

That might disappoint people who love spending time in settings menus, but you're not going to be doing that with CM Security. One potential drawback, however, is that it's relentless in nagging you about other aspects of your device and other apps made by Cheetah that can help you out. But again, it's free, so it's hard to complain too much.



# Figure: CM security App.

**Conclusion:**

# Applications:

Act Mobile makes doing business on mobile devices Data savings, privacy, security & speed on any mobile device, anywhere in the world.

# Top 5 Most secure Phones In The World That Can’t Be Hacked

* + - 1. Bittium Tough Mobile 2C
      2. K-iPhone – One of the most secure Phones
      3. Most secure Phones – Solarin From Sirin Labs
      4. Among the most secure Phones – Purism Librem 5
      5. Sirin Labs Finney U1

|  |  |
| --- | --- |
| **Its pleasure to bring to your attention on the following link which shows the awareness of mobile security**  [**https://www.youtube.com/watch?v=ahNb6kA0Lms**](https://www.youtube.com/watch?v=ahNb6kA0Lms) | **Please Scan the QR-Code.**  C:\Users\Admin\Downloads\Mobile security.png |

# ORAL QUESTIONS:

1. List the components used in the wireless network?
2. What are different mobile security apps?
3. Which facilities are available in the general mobile security application?