Chapter-4: Mobile Telecommunication Technologies, (Network Security and Internet Services)

Learning Objectives:

At the end of this chapter the students will be able to:

- Learn about Mobile Telecommunication Technologies: 1G, 2G, 3G and 4G
- Learn about Network Security Concept such as Threats and prevention from Viruses, Worms, Trojan horse, Spams
- Understand the use of Cookies
- Learn about Firewall
- Learn about India IT Act, Cyber Law, Cyber Crimes, IPR issues, Hacking
- Learn about Web services such as WWW, Hyper Text Markup Language (HTML), eXtensible Markup
- Language (XML); Hyper Text Transfer Protocol (HTTP); Domain Names; URL; Website, Web browser,
- Web Servers; Web Hosting, Web Scripting - Client side (VB Script, Java Script, PHP) and Server side (ASP,JSP, PHP), Web 2.0 (for social networking)

Mobile Telecommunication Technologies

Mobile is a device which is portable. Mobile communication is based on cellular networks. A cellular network is nothing but a radio network. In this network, land is divided into areas called cells. Every cell in the network has a transmitter and a receiver known as cell site or base station. Each cell in the network uses different frequency for the transmission of signals.When joined together these cells provide radio coverage over a large geographical area. The network of cells enables the mobile devices to communicate even if they are moving from one cell to another via base stations.

The last two decades has seen a remarkable growth in the mobile industry both in terms of mobile technology and subscribers.

The first systems offering mobile telephone service were introduced in the late 1940s in the US and in the early 1950s in Europe. These single cell systems were severely constrained by restricted mobility, low capacity, limited service, and poor speech quality. Also the equipment was heavy, bulky, expensive, and susceptible to interference

The use of semiconductor technology and microprocessors made mobile systems smaller, lighter, and more sophisticated.

1G Mobile Systems

The 1G Mobile System was introduced in late 1970s and early 1980s.The 1G mobile system was based on the analog cellular technology. They only had voice facility available and were based on circuit-switched technology. In 1G mobile systems voice was modulated to a frequency of about 150MHz and higher. They used radio towers for transmission. The major drawbacks of the 1G system were its low capacity, poor voice links and no security.

http://www.electronicsforu.com/EFYLinux/efyhome/cover/jun2003/Mobile-tech.pdf

Before discussing about the 2G mobile systems, let's discuss some related terms like

FDMA

It stands for Frequency Division Multiple Access. In this, each user utilizes a portion of the frequency bandwidth available. Each user has its own frequency domain.

CDMA

It stands for Code Division Multiple Access. In this, each user is allocated a unique code sequence. On the sender's end, the data signal is encoded using the given unique code. The receiver decodes the signal according the unique code and recovers the original data.

TDMA

It stands for Time Division Multiple Access. In this, each user is allowed to transmit only within specified time intervals. Different users transmit in different time slots. When users transmit, they occupy the whole frequency bandwidth.

2G Mobile System

The 2G mobile system was introduced in early 1990s. They used digital signals for transmissions of voice. 2G enabled the mobile systems to provide paging, SMS, voicemail and fax services. Both voice and data conversations were digitally encrypted. The 2G system was based on GSM technology. GSM standard was defined by ETSI in 1989. GSM stands for Global System for Mobile Communication. GSM technology is a combination of FDMA and TDMA. With GSM, all subscriber and wireless provider information is stored on interchangeable modules known as SIM (Subscriber Identification Module) cards. By swapping out the SIM card, users can painlessly switch phones or providers. They used circuit switching.

The mobile technology using packet switched domain instead of circuit switched domain were termed as 2.5G mobile systems. They used GPRS (General Packet Radio Service) in addition to GSM. With 2.5G services like MMS, sending pictures through e-mail became possible. GPRS technology was also a major step towards 3G mobile system.

3G Mobile System

The 3G technology adds multimedia facilities to 2G phones by allowing video, audio, and graphics applications. With the advent of 3G technology watching streaming video or video telephony became a reality. The idea behind 3G is to have a single network standard instead of the different types adopted in the US, Europe, and Asia. 3G mobile systems are also known as Universal Mobile Telecommunications System (UMTS) or IMT-2000. They can sustain higher data rates and open the door to many Internet style applications. The main characteristics of IMT-2000 3G systems are:

- A single family of compatible standards that can be used worldwide for all mobile applications.
- Support for both packet-switched and circuit-switched data transmission.
- Data rates up to 2 Mbps (depending on mobility).
- High bandwidth efficiency

4G Mobile System

4G networks will be based on packet switching only. It will be able to support faster transmission. They are projected to provide speeds up to 100 Mbps while moving and 1Gbps while stationary. It is a wireless access technology. 4G can provide better-than-TV quality images and video-links.

Network Security Concepts

Network security deals with policies adopted by network administrator to protect the network from unauthorized access and misuse of network resources. It also ensures that the authorized users have adequate access to all the network resources.

Virus

If you observe that your system

- takes longer time to load applications
- shows unpredictable program behaviour
- shows inexplicable changes in file sizes
- has inability to boot,
- has strange graphics appearing on your screen

This could be because of your computer being infected by a virus.

Virus is a malicious program that attaches itself to the host program. It is designed to infect the host program and gain control over the system without the owner's knowledge. The virus gets executed each

time the host program is executed. Also it has the tendency to replicate. They can spread through external media such as CDs, browsing infected internet sites and from email attachments.

Types of Viruses

- **File Virus:** These viruses infect and replicate when it gets attached to MS-DOS program files with EXE or COM extensions.
- **Boot sector virus:** These viruses infect the boot sector of floppy disks or hard drives. Boot sector of a drive contains program that participates in booting the system. A virus can infect the system by replacing or attaching itself to these programs
- **Macro virus:** These viruses infect and replicate using the MS Office program suite, mainly MS Word and MS Excel. The virus inserts unwanted words or phrases in the document.

Worm

Worm is also a malicious program like a virus. But unlike viruses, it does not need to attach itself to a host program. A worm works by itself as an independent object.It uses security holes in a computer networks to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

Trojan horse

A Trojan horse is a program that contains hidden malicious functions. Trojan Horses trick users into installing them by appearing to be legitimate programs. Once installed on a system, they reveal their true nature and cause damage. Some Trojan horses will contact a central server and report back information such as passwords, user IDs, and captured keystrokes. Trojans lack a replication routine and thus are not viruses by definition.

Spam

The term spam means endless repetition of worthless text. In other words, unwanted messages or mails are known as Spam. At times internet is flooded with multiple copies of the same message, it is nothing but spam. Most spam is commercial advertising. In addition to wasting people's time, spam also eats up a lot of network bandwidth.

Cookies

When the user browses a website, the web server sends a text file to the web browser.This small text file is a cookie. Generally a cookie contains the name of the website from which it has come from and a unique ID tag.

Some cookies last only until the browser is closed. They are not stored on your hard drive. They are usually used to track the pages that you visit so that information can be customised for you for that visit. On the other hand, some cookies are stored on your hard drive until you delete them or they reach their expiry date. These may, for example, be used to remember your preferences when you use the website.

Firewall

A firewall is hardware or software based network security system. It prevents unauthorized access (hackers, viruses, worms etc.) to or from a network.

Firewalls are used to prevent unauthorized internet users to access private networks connected to the Internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. A firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria.

Cyber Crime

Cybercrime is defined as a crime in which a computer and internet is used in an illegitimate way to harm the user. Cyber criminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes. Cybercrimes can be against persons or against property or against the government.

The list of Cyber Crimes includes

- harassment by computer (Cyber Stalking, defamation)
- pornography
- illegal downloads, plagiarism
- software piracy/counterfeiting, copyright violation of software, counterfeit hardware, black market sales of hardware and software, theft of equipment and new technologies
- fraud (credit card fraud, fraudulent use of ATM accounts, stock market transfers, telecommunications fraud), theft of (electronic) money

Cyber Law

Cyber law is an attempt to integrate the challenges presented by human activity on the internet with legal system of laws applicable to the physical world.

There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there has arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology. "INFORMATION TECHNOLOGY ACT, 2000" [ITA-2000] was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of Cyber Crimes. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008].

In the IT Act the word 'computer' and 'computer system' have been so widely defined and interpreted to

mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities and therefore any high-end programmable gadgets like a washing machine or switches and routers used in a network can all be brought under the definition.

Some of the CYBER OFFENCES UNDER THE IT ACT

- Tampering with computer source documents - Section 65
- Hacking -Section 66
- Publishing of information which is obscene in electronic form -Section 67

Intellectual property rights (IPR) Issues

Intellectual property rights are the rights given to an individual over the invention of their own. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.

There are only three ways to protect intellectual property

1. Patents

A Patent is a term used for a specific product designed by an individual. The designer is given exclusive rights over the patent for a limited period of time. With help of the patent right, the owner can stop others from making, using or selling the product design. The owner can take a legal action if someone uses the patent without his/ her permission

In order to obtain a patent, the following conditions should be met:

- The product should be new
- It should be capable of being made or used in some kind of industry
- It should not be a scientific or mathematical discovery
- It should not be a dramatic, musical dramatic or artistic work

2. Trademarks

Trademark can be defined as a name or a different sign or a device identifying a product or a service. The product or the service is produced or provided by a specific person or a company. A Trademark is also known as brand name.It should be officially registered and legally restricted to the use of the specific person or the company.

3. Copyrights

Copyright is the term used for a written document. A legal action can be taken, if copyrights are violated. The following category of work can be considered for copyrights.

- literary works
- musical works, including any accompanying words

- dramatic works, including any accompanying music
- pantomimes and choreographic works
- pictorial, graphic and sculptural works
- motion pictures and other audio visual works
- sound recordings
- architectural works
- computer programs and websites

Hacking

The term hacking was first used at M.I.T during 1950s and 1960s. The term was used for people who engaged themselves in harmless technical experiments and fun learning activities.

A computer enthusiast, who uses his computer programming skills to intentionally access a computer without authorization is known as hacking. The computer enthusiast involved in this activity is known as a hacker. A hacker accesses the computer without the intention of destroying data or maliciously harming the computer.

Another term commonly used with hacking is cracking. Cracking can be defined as a method by which a person who gains unauthorized access to a computer with the intention of causing damage.

Introduction to Web Services

HTML(Hypertext Markup Language)

HTML is language the helps in creating and designing web content. It is a markup language. It has a variety of tags and attributes for defining the layout and structure of the web document. It is designed to display the data in formatted manner. A HTML document has the extension .htm or .html. Hypertext is a text which is linked to another document.

XML (EXtensible Markup Language)

XML is a markup language like HTML. It is designed to carry or store data. In contrast to HTML, it is not designed to display data. Unlike HTML, it does not have predefined tags. It is possible to define new tags in XML. It allows the programmer to use customized tags. XML is case sensitive. XML is deigned to be self-descriptive. XML is a W3C recommendation.

XML documents form a tree structure.

For Example

<root>

<child>

<subchild>.....</subchild>

</child>
</root>

WWW (World Wide Web):

WWW can be defined as a hypertext information retrieval system on the Internet. Tim Berners -Lee is the inventor of WWW. WWW is the universe of the information available on the internet.

WWW consists of web pages, which use HTML to interchange information on the internet. All the webpages on WWW use HTTP transfer protocol for any information with the capability for making hypertext jumps

Web page

Web page is an electronic document designed using HTML. It displays information in textual or graphical form. It may also contain downloadable data files, audio files or video files. Traversal from one webpage to another web page is possible through hyperlinks.

A web page can be classified into two types:

Static web page: A web page which displays same kind of information whenever a user visits it, is known as a static web page. A static web page generally has.htm or .html as extension

Dynamic web page: An interactive web page is a dynamic webpage. A dynamic web page uses scripting languages to display changing content on the web page. Such a page generally has php, .asp," or .jsp as extension.

A scripting language is a programming language which can be embedded or integrated with other languages. Some of the most widely used scripting languages are JavaScript, VBScript, PHP, Perl, Python, Ruby, and ASP. They have been used extensively to create dynamic web pages.

Dynamic web pages support two types of scripting:

- **Client-Side Scripting**

  On some web pages the contents change in response to an action done by the user, for example a click from the mouse or a key press from a keyboard action. Such pages use client-side scripting. In this technology, the content is generated on the user's local computer. VB Script and Java Script are examples of client-side scripting languages.

- **Server -Side Scripting**

  Some web pages use applications running on the server to generate the web content. Such pages use server-side scripting language. Web page display the current time and date, forums, submission forms, shopping carts etc., use server-side scripting. ASP,JSP, PHP are examples of server-side scripting languages.

Website: Related webpages from a single wen domain is termed as a website. A website has multiple

webpages providing information about a particular entity.

Web browser

Web browser is software program to navigate the web pages on the internet. A bowser interprets the coding language of the web page and displays it in graphic form. A web browser allows anyone to access the web without even knowing commands used in software languages to design a web page.

Internet works on client -server model. A web browser is a client which requests the information from the web server. The web server sends the information back to the client. The web address of the webpage written on the address bar tells the web browser which page to access.

Web Browser is of two types:

- Text based browsers
- Graphical browsers

URL (Uniform resource locator)

Web address of the web page written on the address bar of the browser is known as the uniform resource locator (URL). A URL is a formatted text string used to identify a network resource on the Internet. Network resources are files that can be plain Web pages, text documents, graphics, downloadable files, services or programs. Every network resource on the web has a unique URL.

The URL text string consists of three parts:

- network protocol
- host name or address
- file or resource location

The textstring of a URL has the following format:

protocol://server/path/resource

Network Protocol

The network protocol substring identifies the protocol to be used to access the network resource. These strings are short names followed by the three characters '://' . Other examples of protocols include http, gopher, wais, ftp and mailto.

URL Host/Server

The host name or address substring identifies the host/server that holds the resource. Hosts names are sometimes called domain names. For example: www. School.com is a domain name

Host names are mapped into numeric IP addresses. The domain name www.school.com may have IP address 192.2.100.1. An IP address is a binary number that uniquely identifies computers and other devices on a TCP/IP network. Services in the name of one host can be provided by many servers, which have

different IP addresses. One server, with one IP address, can provide services in the name of many hosts. So there is not a one-to-one relationship between host name and IP address. It is more convenient for the user to remember a numeric IP address than the domain name.

Host names are mapped to IP addresses by a server known as a DNS server, or domain nameserver. DNS stands for Domain Name Service. In a large network, many DNS servers may collaborate to provide the mapping between host names and IP addresses.

URL Resource Location

The file or resource location substring contains a path to one specific network resource on the host/server.Resources are normally located in a host directory or folder.

For example:www.school.com/syllabus/preprimary/nursery.htm is the location of this Web page including two subdirectories and the file name.

When the location element is omitted such as in http:// www.school.com/, the URL conventionally points to the root directory of the host and often a home page.

Web Server

A Web server is a computer or a group of computers that stores web pages on the internet.

It works on client/server model. It delivers the requested web page to web browser. Web servers use special programs such as Apache or IIS to deliver web pages over the http protocol.

Each server has a unique IP address and domain name. In order to access a webpage, the user writes the URL of the site on the address bar of the browser.The machine on which the browser is running sends a request to the IP address of the machine running the web server for that page. Once the web server receives that request, it sends the page content back to the IP address of the computer asking for it. The web browser then translates that content into all of the text, pictures, links, videos, etc.

A single web server may support multiple websites or a single website may be hosted on several linked servers.

Web hosting

Web hosting is the process of uploading/saving the web content on a web server to make it available on WWW. In case a individual or a company wants to make its website available on the internet, it should be hosted on a web server.

Web 2.0

The term web 2.0 was given by O'Reilly Media in 2004. Web 2.0 refers to new generation of dynamic and interactive websites. Web 2.0 websites uses a new programming language called AJAX (Asynchronous JavaScript and XML). AJAX helps a dynamic website connect to the web server and download small

amount of data based on the interaction with the user. In this technology only the part of the website which is updated is reloaded. The entire page does not get reloaded each time. This helps in making the website interactive.

Applications supported by web 2.0 are as followings:

- blogging
- social bookmarking
- RSS
- wikis and other collaborative applications
- interactive encyclopaedias and dictionaries
- Advanced Gaming

LETS REVISE

1G Mobile Systems: The 1G Mobile System was introduced in late 1970s and early 1980s.The 1G mobile system was based on the analog cellular technology. They only had voice facility available.

2G Mobile Systems: They used digital signals for transmissions of voice. 2G enabled the mobile systems to provide paging, SMS, voicemail and fax services.

3G Mobile Systems: The 3G technology adds multimedia facilities to 2G phones by allowing video, audio, and graphics applications.

4G Mobile Systems: 4G will provide better-than-TV quality images and video-links.

Virus: Virus is a malicious program that attaches itself to the host program. It is designed to infect the host program and gain control over the system without the owner's knowledge.

Worm: Worm is also a malicious program like a virus. But unlike viruses, it does not need to attach itself to a host program. A worm works by itself as an independent object.

Trojan horse: A Trojan horse is a program that contains hidden malicious functions. Trojan Horses trick users into installing them by appearing to be legitimate programs.

Spam: The term spam means endless repetition of worthless text. In other words, unwanted messages or mails are known as Spam.

Cookies: This small text file is a cookie. Generally a cookie contains the name of the website that it has come from and a unique ID tag.

Firewall: A firewall is hardware or software based network security system. It prevents unauthorized access (hackers, viruses, worms etc.) to or from a network.

Cyber Crime: Cybercrime is defined as a crime in which a computer and internet is used in an illegitimate way to harm the user.

Cyber Law: Cyber law is an attempt to integrate the challenges presented by human activity on the internet with legal system of laws applicable to the physical world.

Intellectual property rights are the rights given to an individual over the invention of their own. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time

Intellectual property rights (IPR) Issues: Intellectual property rights are the rights given to an individual over the invention of their own. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.There are only three ways to protect intellectual property

- Patents
- Copyrights

2 Trademark

Hacking: The term was used for people who engaged themselves in harmless technical experiments and fun learning activities.

Cracking: Cracking can be defined as a method by which a person who gains unauthorized access to a computer with the intention of causing damage.

HyperText Transfer Protocol (HTTP): HTTP is the protocol that is used for transferring hypertext (i.e. text, graphic, image, sound, video etc.) between two computers and is particularly used on the World Wide Web. It is a TCP/IP based communication protocol and provides a standard for Web browsers and servers to communicate.

WWW (World Wide Web): WWW can be defined as a hypertext information retrieval system on the Internet. Tim Berners -Lee is the inventor of WWW. WWW is the universe of the information available on the internet.

Web page: Web page is an electronic document designed using HTML. It displays information in textual or graphical form. It may also contain downloadable data files, audio files or video files.

A web page can be classified into two types:

- Static web page
- Dynamic web page

Website: Related webpages from a single wen domain is termed as a website. A website has multiple webpages providing information about a particular entity.

Web browser: Web browser is software program to navigate the web pages on the internet. A bowser interprets the coding language of the web page and displays it in graphic form.

URL (Uniform resource locator): Web address of the web page written on the address bar of the browser is known as the uniform resource locator (URL).

Web hosting: Web hosting is the process of uploading/saving the web content on a web server to make it available on WWW.

Web 2.0: Web 2.0 refers to new generation of dynamic and interactive websites. Web 2.0 websites uses a new programming language called AJAX (Asynchronous JavaScript and XML).