# E – Content

## Subject - Information Security and Cyber Laws

**B.Tech (Information Technology) 3rd Year 5th Sem**

Mr. Krishna Kumar Yadav

# INFORMATION SYSTEM

Information system is a system which is used for organizing and processing information, generally computer-based. Also, it is a useful system within a business because it manages the development and operations of the business's information. The importance of information systems are growing. As data is now taking towards a digital form, instead of just a paper-based. Its good point is that the data is becoming readily available and become more secure. It prevents the data from unauthorized access. Like in hospitals information systems are very helpful, your data is stored in computers and where ever you are in the hospital your details are available at a few key strokes.

An information system (IS) is any combination of information technology and people's activities using that technology to support operations, management, and decision-making. In a very broad sense, the term *information system* is frequently used to refer to the interaction between people, algorithmic processes, data and technology. In this sense, the term is used to refer not only to the information and communication technology (ICT) an organization uses, but also to the way in which people interact with this technology in support of business processes.

An information system is a work system whose activities are devoted to processing (capturing, transmitting, storing, retrieving, manipulating and displaying) information. An information system is a mediating construct between actions and technology.
As such, information systems inter-relate with data systems on the one hand and activity systems on the other. An information system is a form of communication system in which data represent and are processed as a form of social memory. An information system can also be considered a semi-formal language which supports human decision making and action.

## IMPORTANCE OF INFORMATION SYSTEM:

Information system is a foundation for conducting business today. In many businesses, survival and the ability to achieve strategic business goals is difficult without extensive use of information technology.
There are six reasons or objectives why businesses use information system:

1. Operational excellence,
2. New products, services, and business models,
3. Customer and supplier intimacy,
4. Improved decision making,
5. Competitive advantage and
6. Survival.

**1. OPERATIONAL EXCELLENCE.** Business improves the efficiency of their operations in order to achieve higher profitability. Information systems are important tools available to managers for achieving higher levels of efficiency and productivity in business operations. A good example is Wal-Mart that uses a Retailing system, which digitally links its suppliers to every one of Wal-Mart's stores. As soon as a customer purchase an item, the supplier is monitoring the item, knows to ship a replacement to the shelf.

2. **NEW PRODUCTS, SERVICES, AND BUSINESS MODELS.** Information system is a major tool for firms to create new products and services, and also an entirely new business

models. A business model describes how a company produces, delivers, and sells a product or service to create wealth.
Example: Apple Inc transformed an old business model based on its iPod technology platform that included iPod, the iTunes music service, and the iPhone.

3. **CUSTOMER/SUPPLIER INTIMACY**. When a business serves its customers well, the customers generally respond by returning and purchasing more. This raises revenue and profits. The more a business engages its suppliers, the better the suppliers can provide vital inputs. Example: The Mandarin Oriental in manhattan and other high-end hotels exemplify the use of information systems and technology to achieve customer intimacy. They use computers to keep track of guests' preferences, such as their preffered room temperature, check-in time, and television programs.

4. **IMPROVED DECISION MAKING.** Many managers operate in an information bank, never having the right information at the right time to make an informed decision. These poor outcomes raise costs and lose customers. Information system made it possible for the managers to use real time data from the marketplace when making decision. Example: Verizon Corporation uses a Web-based digital dashboard to provide managers with precise real -time information on customer complains, network performance.. Using this information managers can immediately allocate repair resources to affected areas, inform customers of repair efforts and restore service fast.

5. **COMPETITIVE ADVANTAGE.** When firms achieve one or more of these business objectives (operational excellence, new products, services, and business models, customer/supplier intimacy, and improved decision making) chances are they have already achieved a competitive advantage. Doing things better than your competitors, charging less for superior products, and responding to customers and suppliers in real time all add up to higher sales, and higher profits. Example: Toyota Production System focuses on organizing work to eliminate waste, making continues improvements, TPS is based on what customers have actually ordered.

6. **DAY TO DAY SURVIVAL**. Business firms invest in information system and technology because they are necessities of doing business. These necessities are driven by industry level changes. Example: Citibank introduced the first automatic teller machine to attract customers through higher service levels, and its competitors rushed to provide ATM's to their customers to keep up with Citibank. Providing ATMs services to retail banking customers is simply a requirement of being in and surviving in the retail banking business. Firms turn to information system and technology to provide the capability to respond to these.

## CHANGING NATURE OF INFORMATION SYSTEM:

In the past decade, the nature of IS has undergone a dramatic change, from mainframe-based IS to client / server computing to today's web-based information system, with the Internet having made the revolution.

The four powerful worldwide changes that have altered the business environment are:
1. Globalization;
2. Rise of the information economy;
3. Transformation of the business enterprise;
4. Emergence of the digital firm.

# DISTRIBUTED INFORMATION SYSTEM:

Distributed information system is defined as, "A number of independent computers linked by a network for shearing the information among them". A Distributed computing is a field of computer science that studies distributed information systems. A distributed information system consists of multiple autonomous computers that communicate or exchange of the information through a computer network. The computers interact with each other in order to achieve a common goal (information). A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs.

There is no single definition of a distributed system; the following defining properties are commonly used:

- There are several autonomous computational entities (***computers*** **or** ***nodes***), each of which has its own local memory.
- The entities communicate with each other by message passing or transferring the information.

The study of distributed computing became its own branch of computer science in the late 1970s and early 1980s. The first conference in the field, Symposium on Principles of Distributed Computing (PODC), dates back to 1982, and its European counterpart International Symposium on Distributed Computing (DISC) was first held in 1985.

Examples of distributed information systems and applications of distributed computing include the following:

- Telephone networks and cellular networks
- Computer networks such as the Internet.
- Wireless sensor networks.
- Routing algorithms
- Distributed databases and distributed database management systems
- Industrial/ Aircraft control systems.

## ARCHITECTURE OF DISTRIBUTED INFORMATION SYSTEM:

Various hardware and software architectures are used for distributed information system or distributed computing. At a lower level, it is necessary to interconnect multiple CPUs with some sort of network, regardless of whether that network is printed onto a circuit board or made up of loosely-coupled devices and cables. At a higher level, it is necessary to interconnect processes running on those CPUs with some sort of communication system.

Distributed programming typically falls into one of several basic architectures or categories: client–server, 3-tier architecture, *n*-tier architecture or tight coupling.

1. **Client–server:**

Smart client code contacts the server for data then formats and displays it to the user. Input at the client is committed back to the server when it represents a permanent change.

2. **3-tier architecture:**

Three tier systems move the client intelligence to a middle tier so that stateless clients can be used. This simplifies application deployment. Most web applications are 3-Tier.

3. ***n*-tier architecture:**

*n-tier* refers typically to web applications which further forward their requests to other enterprise services. This type of application is the one most responsible for the success of application servers.

4. **Tightly Coupled (Clustered):**

Typically to a clusters of machines that closely work together, running a shared process in parallel. The task is subdivided in parts that are made individually by each one and then put back together to make the final result.

5. **Loosely Coupled Systems:**

Loosely coupled clusters are a group of machines which can operate independent of each other. Communications between nodes (or sub-clusters) is often done via a queuing system. Loosely coupled systems use components that were not necessarily intended specifically for use in such systems.

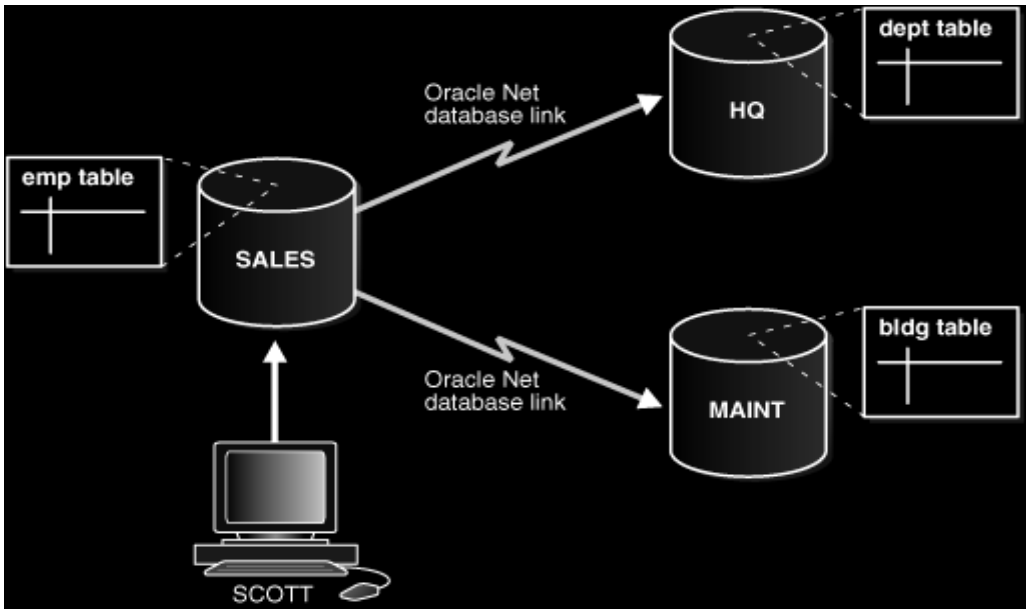



**Fig 1: Distributed Information System**

## NEED OF DISTRIBUTED INFORMATION SYSTEM:

Business competitions and pressures are rising today at a very rapid speed. In the success of digital economy led by e-business, we find three 'mantras' of success:

Liberalization,

Privatization,

Globalization

Mobile commerce has made the business free from geographical boundaries. Data and information are the vital corporate assets and information security is crucial as businesses make knowledge based decisions. We certainly do not want the confidential data and information to be leaked outside the required boundaries.

It is important to note that while the industrial age witnessed great developments in terms of engineering, a significant dimension, connectivity was missing. Producers and consumers of goods all remained disparate and unconnected, without knowing how the others were transacting their businesses. This isolation is not true in today's scenario since we have a new way of doing business known as electronic business or 'e-business'.

In the modern days, information system handling information in all forms, not just the text-based data that came in flat files but also the rich text, images/graphics and voice. The widening scope of information system is summarized as follows:

1. 1950s – Technical Changes
2. 1960s-1970s – Managerial Control
3. 1980s-1990s – Institutional core activities
4. Today – Digital information webs extending beyond the enterprise.

Thus, today is the era of the 'extended enterprise' which serves the needs of networked enterprise, the information system are no more confined to a single location, single computer.

## ADVANTAGES OF DIS:

1. Each user has control of his own equipment, to a reasonable degree.
2. Each user can add his own programs at their own leisure.
3. Sometimes cheaper up front capital cost.

## DISADVANTAGES OF DIS:

1. Typical lifespan of 3 years.
2. Many moving parts (fans, hard drives) which are susceptible to failure.
3. Large vulnerability to security threats (both internal and external).
4. Usually has higher cost of ownership, when measured over 3+years.

# INTERNET

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANet. The original aim was to create a network that would allow users of a research computer at one university to be able to "talk to" research computers at other universities. A side benefit of ARPANet's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

## ROLE OF INTERNET IN INFORMATION SYSTEM:

The Internet has enabled entirely new forms of social interaction, activities, and organizing, thanks to its basic features such as widespread usability and access. Social networking websites such as Facebook, Twitter and MySpace have created new ways to socialize and interact. Users of these sites are able to add a wide variety of information to pages, to pursue common interests, and to connect with others. It is also possible to find existing acquaintances, to allow communication among existing groups of people. Sites like Linked In foster commercial and business connections. YouTube and Flickr specialize in users' videos and photographs.

With the use of internet, it is possible to transmit/receive information containing images, graphics, sound and videos. ISP (Internet services provider) industry can offer services as:

- Linking consumers and businesses via internet.
- Monitoring/maintaining customer's Web sites.
- Network management/systems integration.
- Backbone access services for other ISP's.
- Managing online purchase and payment systems.

The internet is designed to be indefinitely extendible and the reliability of internet primarily depends on the quality of the service providers' equipments.

## BENEFITS OF INTERNET:

There are many benefits of internet such as:

- Doing fast business.
- Trying out new ideas.
- Gathering opinions.

- Allowing the business to appear alongside other established businesses.
- Improving the standards of customer service/support resource.
- Supporting managerial functions.

## LIMITATIONS OF INTERNET:

- Security
- Privacy
- Threats: Hackers, Viruses etc.

## WEB SERVICES

A **Web service** is a method of communication between two electronic devices over a network.

Web Services are a general model for building applications and can be implemented for any operation system that supports communication over the Internet. Web services take advantage of the best of component-based development. Component-based object models like Distributed Component Object Model (DCOM), Remote Method Invocation (RMI), and CORBA's Internet Inter-ORB Protocol (IIOP) have been around for some time. Unfortunately, they depend on an object model–specific protocol. Web services extend these models by communicating with Simple Object Access Protocol (SOAP) and XML to eradicate the barrier posed by the object model–specific protocol.

The evolution of SOAP has expanded the boundaries of the Internet. SOAP and HTTP enable you to log on to external systems and execute remote function calls. Using a Web browser in Melbourne, Australia, for example, you can execute methods on your company's mainframe in Seattle, Washington. This architecture enables Web servers to work in tandem to expose their business logic without compromising security.

Web services work by basically using HTTP and SOAP to make business data available on the Web. Web services expose business objects (COM objects, JavaBeans, etc.) to SOAP calls over HTTP and execute remote function calls. That way, Web service consumers are able to invoke method calls on remote objects by using SOAP and HTTP over the Web.

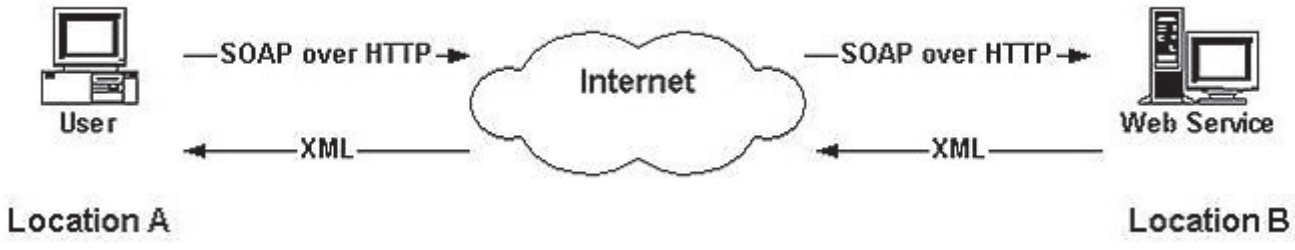



**Fig 1: Basic structure of a Web service.**

**Figure (1)** shows you what I'm trying to explain. It's the basic structure of a Web service. The user at Location A uses the Internet as a vehicle to execute remote function calls (RFCs) on Location B's Web server. The communication is done using SOAP and HTTP.

How is the user (consumer) at Location an aware of the semantics of the Web service at Location B? This question is answered by conforming to a common standard. Service Description Language (SDL), SOAP Contract Language (SCL), and Network Accessible Specification Language (NASSL) are some XML-like languages built for this purpose. Recently, IBM and Microsoft came together and agreed on Web Service Description Language (WSDL) as the Web service standard.

**The W3C states, we can identify two major classes of Web services:**

**REST (Representational State Transfer)-compliant Web services:** In which the primary purpose of the service is to manipulate XML representations of Web resources using a uniform set of "stateless" operations.

**Arbitrary Web services:** In which the service may expose an arbitrary set of operations."

## How Do Clients Communicate with Web Services? (Read)

Does Location A's user actually execute methods on Location B's Web servers? That's what I asked myself when I was new to this technology. As you can imagine, that could pose a serious security threat. As Webmasters, we don't want anyone to use our Web resources and do malicious damage to our sensitive data—not to mention chewing up our bandwidth. We also have to remember that this is a distributed application. Therefore we have to be concerned about the marshalling of data.

To get around the security and data marshalling problems, we need to replicate the object behavior locally on the user's Web server. In this example, we will replicate Location B's Web service functionality at Location A. That means creating a *proxy object* to act on behalf of the original Web service. The proxy object will have all the publicly available data interfaces as the original Web service. But how do we get these interfaces?

The publicly available data interfaces are declared with the "Web Only" directive in the Web service's code; every "Web Only" method will be replicated at the proxy object. This protects us from exposing sensitive business logic to malicious hackers at the Web service end (Location B). The best implementation will be a thin Web proxy object class that delegates sensitive process to a back end. In a way, what we are doing is synchronizing object data exchanges between Locations A and B. This process is known as creating a proxy object at Location A.

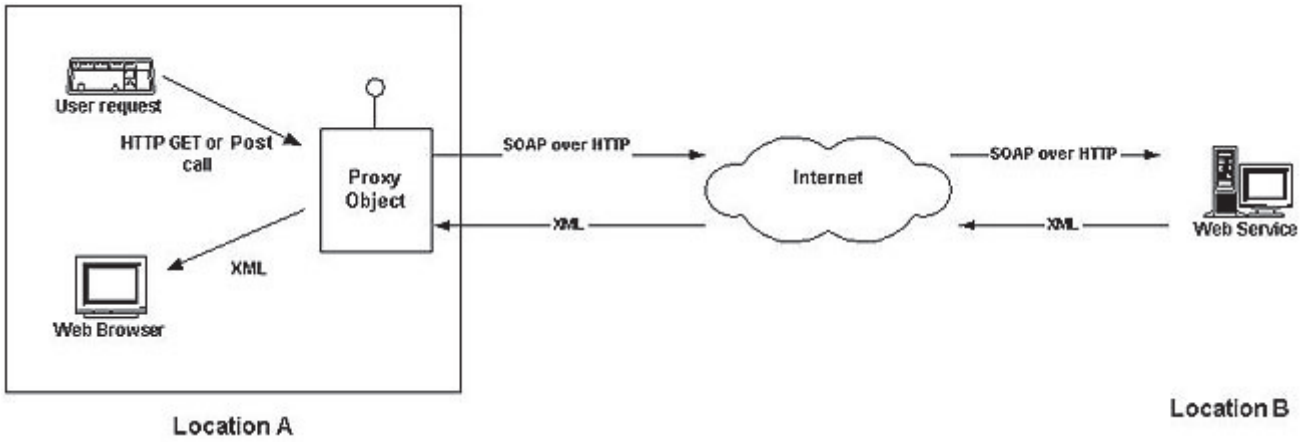



**Fig 2. Structure for client communicate to web-services**

The code at Location A instructs the proxy object. Then the proxy object associates with Location B's Web service and produces the results to users at Location A. Figure 2 shows the communication between a Web browser client and a Web service over the Internet.

Because the proxy object is the basic concept of the Web service invocation, the first step in creating a Web service client is to create a proxy object (see link below). Then you can use multiple platforms (Web browsers, WAP clients, PDAs, and SOAP clients) to extract data from the proxy object.

## INFORMATION SYSTEM THREATS

A threat is anything (man made or act of nature) that has the potential to cause of harm.

A threat is also defined as "A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability".

Threat modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. In this context, a threat is a potential or actual adverse event that may be malicious (such as denial-of-service attack) or incidental (such as the failure of a storage device), and that can compromise the assets of an enterprise.

## CLASSIFICATION OF SECURITY THREATS:

In order for one to produce a secure system, it is important to classify threats. The classification of threats could be:

1. Physical threats,
2. Accidental error,
3. Unauthorized access,
4. Malicious misuse.

1. **PHYSICAL THREAT:**

Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software, theft of the computer system, vandalism, natural disaster such as flood, fire, war, earthquakes etc. Acts of terrorism such as the attack on the world trade centre is also one of the major threats to computer which can be classified as physical threat.

Another good example of a physical threat to computer system is the flooding of the city of New Orleans (Hurricane Katrina) during which valuable information was lost and billions of computer data were destroyed.

2. **ACCIDENTAL ERROR:**

This is also an important security issue which computer security experts should always put into consideration when designing security measures for a system. Accidental errors could occur at any time in a computer system but having proper checks in place should be the major concern of the designer. Accidental error includes corruption of data caused by programming error, user or operator errors.

3. **UNAUTHORIZED ACCESS:**

Dada stored on the computer system has to be accessed for it to be translated into useful information. This also poses a great security threats to the computer system due to unauthorized person's having access to the system. Not only this, information can be accessed via a remote system in the process of being transmitted from one point to the other via network media which includes wired and wireless media. Considering an example of an organization in which a member of staff at a particular level of hierarchy within the establishment is only allowed access to specific area according to the policy of the organization. If these employees by other means not set in the organization policy gain access to the restricted data area on the computer, this can be termed an unauthorized access.

4. **MALICIOUS MISUSE:**

Any form of tampering of the computer system which includes penetration, Trojan horses' viruses and any form of illegal alteration of the computer system which also includes the generation of illegal codes to alter the standard codes within the system can be termed as malicious misuse. This could also lead to a great financial loss and should be prevented in all cases.

# INFORMATION SYSTEM ATTACKS:

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Attacks are classified in two categories such as:

1. Passive attacks

2. Active attacks

## PASSIVE ATTACKS:

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

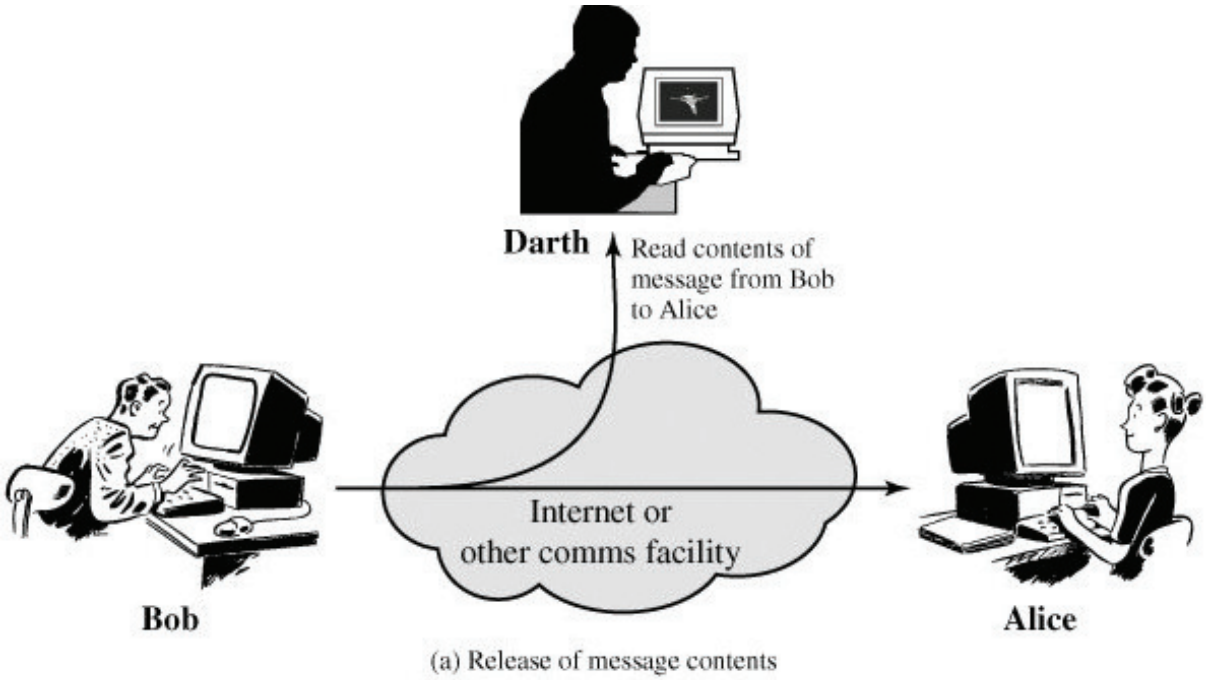
Two types of passive attacks:

a. Release of message contents
b. Traffic analysis.

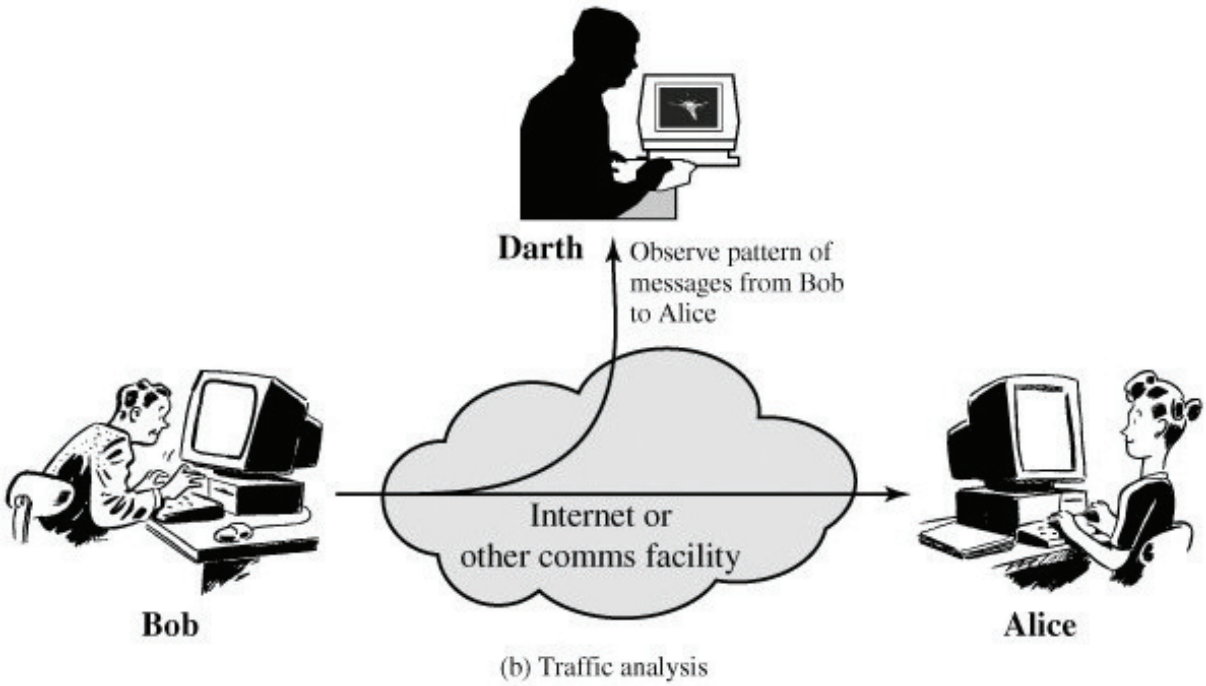
**Release of message (fig 3.a)** contents is a telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

**Traffic analysis (fig 3.b)** is when the third person observes the pattern of the message from sender to receiver.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is not sent and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.




(a) Release of message contents




(b) Traffic analysis

**Fig 3. Passive attacks**

## ACTIVE ATTACKS:

An active attack attempts to alter system resources or affect their operation. Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

**Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

**Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 1.4c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure 1.4d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

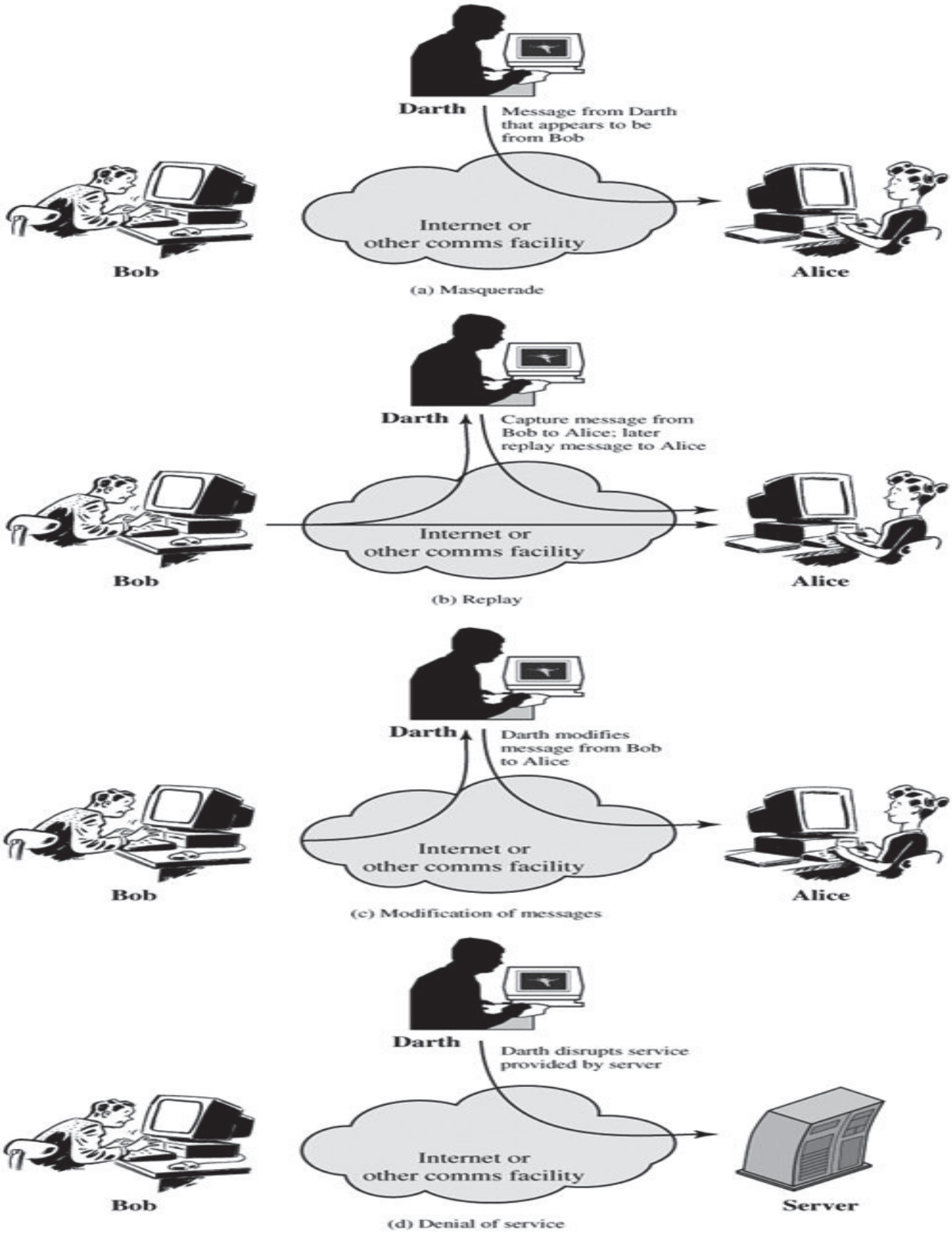



**Figure 1.4. Active Attacks**

# INFORMATION SECURITY:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is the process of protecting the information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing.

Many businesses are solely based on information stored in computers. Personal staff details, client lists, salaries, bank account details, marketing and sales information may all be stored on a database. Without this information, it would often be very hard for a business to operate. Information security systems need to be implemented to protect this information.

Effective information security systems incorporate a range of policies, security products, technologies and procedures. Software applications which provide firewall information security and virus scanners are not enough on their own to protect information. A set of procedures and systems needs to be applied to effectively deter access to information.

Information security has held as a basic principal of information security are:

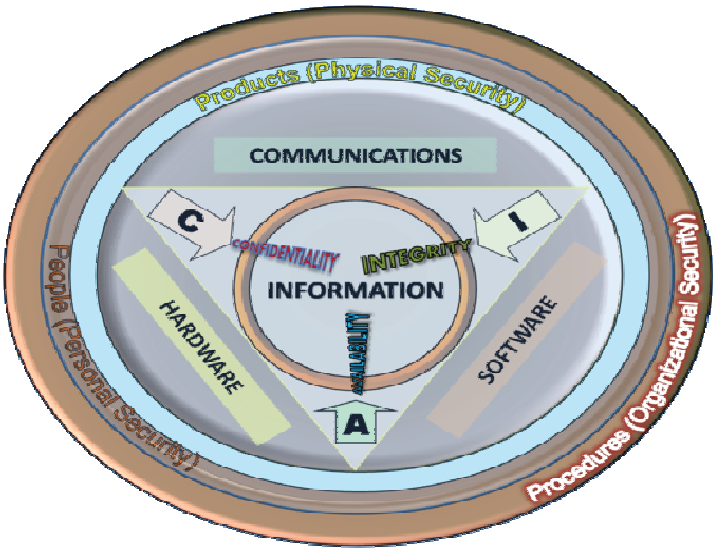
1. Confidentiality,
2. Integrity and
3. Availability

## 1. CONFIDENTIALITY:

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.
Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

## 2. INTEGRITY:

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.




**(Or)**

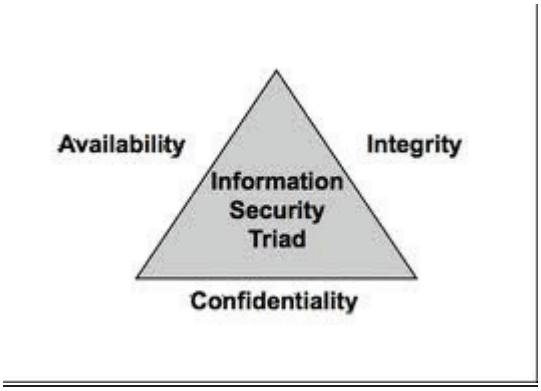



**Fig: Basic principal of Information Security**

### 3. AVAILABILITY:

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

# LAPTOP

As an impact of the reduction in the process of computing technology, laptop has become very common in use. The wireless capability has enhanced the business functions and mobile access to information anytime and anywhere but poses a large threat to business function security due to its mobility. According to the computer security industry and insurance company statistics, thefts of laptop have always been a major issue. Criminals are targeting laptops as they are expensive and profit can be made easily. Few laptop thieves are actually interested in the information stored in them. Most laptop contains personal and corporate information that can be sensitive and may be misused by an unauthenticated and malicious user. So it is necessary and critical to protect the laptops and the information stored in these laptops. Below we present some basic security principles that need to be implemented to protect laptops and the sensitive information contained in them.

## BASIC SECURITY PRINCIPLES FOR LAPTOP:

### 1. CHOOSE A SECURE OPERATING SYSTEM AND LOCK IT DOWN:

To care about your data, you must pick an operating system that is secure. Windows 2000 professional and Windows XP professional both offer secure logon, file level security, and the ability to encrypt data. Such type of security is not provided by Windows 95/98/ ME etc., if you are running any of them, anyone who pick up your laptop can access your data.

### 2. ENABLE A STRONG BIOS PASSWORD:

Security begins right from the start by password protecting the BIOS, some laptop manufacturers use stronger BIOS protection schemes than others, so you should find out from your laptop manufacturer what the procedure is for resetting the BIOS password. If they absolutely demand that you send it back into the factory and don't give you a "workaround", you have a better chance of recovering the machine and may be even catching the thief (Both IBM and Dell provide this feature). Also find out if the BIOS password locks the hard drive so it can't simply be removed and reinstalled into a similar machine.

### 3. ENGRAVE THE LAPTOP:

Permanently marking the outer case of the laptop with your company name, address, and phone number may greatly increase your odds of getting it returned to you if carelessly leave it in a hotel room or somewhere else. According to the FBI, 97% of unmarked computers are never recovered. Marking may also prevent it from simply being resold over the internet via an online auction.

## 4. REGISTER THE LAPTOP WITH THE MANUFACTURER:

Most of use is in a habit of throwing away the registration cards for all of the electronic items we buy every day, because we have learned that it just leads to more junk mail. Registering your laptop with the manufacturer will "flag" it if a thief ever sends it in for maintenance, and increases your chances of getting it back. It also pays to write down your laptop's serial number and store it in a safe place. In the event your laptop is stolen, it will be impossible for the police to ever recover it if they can't trace it back to you.

## PRINCIPLE OF PHYSICAL SECURITY OF LAPTOP:

### 1. GET A CABLE LOCK AND USE IT:

Over 80% of the laptop on the market is equipped with a **Universal Security Slot** (USS) that allows them to be attached to a cable lock or laptop alarm. Although this may not stop determined thieves with bolt cutters, it can effectively keep the casual thieves away who generally take advantage of you while you're sleeping in an airport lobby, leaving it on a table to go the bathroom, etc. These devices are not very costly and can be found at office supply stores or online. Tubular locks are preferable to common tumbler lock design.

### 2. USE A DOCKING STATION:

Almost 40% of laptop theft occurs in the office. Poorly screened housekeeping staff, contractors, and disgruntled employees are the usual suspects. You can help prevent this by using a docking station that is permanently affixed to your desktop and has a feature which locks the laptop securely in place. If you need to leave it overnight, or for the weekend, lock your laptop in a secure filling cabinet in your office and lock your office door.

### 3. LOCK UP YOUR PCMCIA CARDS:

Apart from locking your PC to desk with a cable lock to keep someone from walking away with your laptop; you can do something to keep someone from stealing the PCMCIA NIC card or modem that is sticking out of the side of your machine. When not in use, eject these cards from the laptop bay and lock them in a safe place. Even when they are not being used, PCMCIA card still consume battery power and contribute to the heat levels within your laptop while they are left inserted into their slots.

### 4. USE A PERSONAL FIREWALL ON YOUR LAPTOP:

It is a popular practice for the corporate networks to protect their servers and workstations by configuring a firewall to prevent intruders from hacking their system via the company's internet connection. But once users leave the corporate buildings and connect to the web from home or other places, their data is vulnerable to attack. Personal firewalls such as ***BlackIce*** and ***ZoneAlarm*** are an effective and inexpensive layer of

security that takes only a few minutes to install. The use of a good third-party personal firewall to secure your Windows XP workstations in recommended.

5. **USE TRACKING SOFTWARE TO HAVE YOUR LAPTOP CALL HOME:**

There are a number of vendors that offer stealthy software solutions that enable your laptop to check in to a tracking center periodically using a traceable signal. In the event your laptop is lost or stolen, these agencies work with the police, Phone Company and internet service providers to track and recover your laptop. CompuTrace, SecureIT, Stealth Signal, and ZTrace provide tracking services for corporations and individuals.

## PROTECTING YOUR SENSITIVE DATA:

1. **USE THE NTFS FILE SYSTEM:**

Assuming you are using Windows NT/2000/XP on your laptop, use the NTFS file system to protect your data from laptop thieves who may try to access your data. FAT and FAT32 file system do not support file level security and give hackers a big wide open door to your system.

2. **DISABLE THE GUEST ACCOUNT:**

Although Windows 2000 disables the guest account by default but you should check to make sure the guest account is not enabled. For additional security assign a complex password to the account anyway, and restrict its logon 24*7.

3. **RENAME THE ADMINISTRATOR ACCOUNT:**

Although hackers may use the SID (Society for Innovation and Development) to find the name of the account and hack that, but renaming the Administrator account will some amateur hackers and will annoy the more determined ones. Remember that hackers won't know what the inherit or group permissions are for an account, so they will try to hack any local account they find and then try to hack other accounts as they go to improve their access. If you rename the account, try not to use the word 'Admin' in its name. Pick something that may not reveal that it has right to anything.

4. **ENABLE EFS (ENCRYPTING FILE SYSTEM):**

Windows 2000 ships with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This helps prevent a hacker from accessing your files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on folders, not just files. This way, all files that are placed in that are placed in that folder will be encrypted.

## 5. DISABLE THE INFRARED PORT ON YOUR LAPTOP:

The hacker may use the Infra Red (IR) port to browse someone else's files from across a conference room table without them knowing it. You can disable the IR port via the BIOS, or can simply cover it up with a small piece of black electrical tape.

## MOBILE COMPUTING

Mobile computing is defined as, ***"A technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link".***
Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution to the biggest problem of business people on the move – mobility.

### MOBILE COMPUTING consists of several things such as:

1. Mobile computing requires, wireless network to support outdoor mobility and handoff from one network to the next at a pedestrian or vehicular speed.

2. Mobile computing about both physical and logical computing entities that move.
    a. Physical entities are computers that change locations.
    **b.** Logical entities are instances of a running user application or a mobile agent.
3. Mobile agents can migrate any where over internet.
4. Mobility originated from the desire to move either toward resources or away from scarcity.
5. Mobile computing is Ubiquitous computing or pervasive computing that refers to access to computer network all the time at any location by any person.
6. Traveler in car using laptop connected with a GSM phone - engaged in mobile computing.

### CHALLENGES OF MOBILE COMPUTING:

1. Physical location of mobile is not the network address, so how do we route the message to a mobile host.
2. Cellular community's effort based on location management of cellular phone users.
3. TCP works is unsuitable for wireless network as it interprets errors as packet loss.
4. ITCP (Indirect TCP) splits TCP into two parts:
    - One between sender and local MSS of the recipient.
    - The other between local MSS and recipient.
    - If MH switches cell during life time of a ITCP connection center point of connection oves to new MSS, sender remains completely unaware about it.
5. Published data is filtered by client and server provides directory information for assisting the filtering.
6. Handoff management - an MH moves from one cell to another while being connected.

7. Conventional model will not work.
8. Two-tier transaction.
9. Security is a major concern.
10. Authentication schemes.
11. Encryption schemes.

## APPLICATION OF MOBILE COMPUTING:

The importance of Mobile Computers has been highlighted in many fields of which a few are described below:

- **FOR ESTATE AGENTS**

  Estate agents can work either at home or out in the field. With mobile computers they can be more productive. They can obtain current real estate information by accessing multiple listing services, which they can do from home, office or car when out with clients. They can provide clients with immediate feedback regarding specific homes or neighborhoods, and with faster loan approvals, since applications can be submitted on the spot. Therefore, mobile computers allow them to devote more time to clients.

- **EMERGENCY SERVICES**

  Ability to receive information on the move is vital where the emergency services are involved. Information regarding the address, type and other details of an incident can be dispatched quickly, via a CDPD system using mobile computers, to one or several appropriate mobile units which are in the vicinity of the incident.

- **IN COURTS**

  Defense counsels can take mobile computers in court. When the opposing counsel references a case which they are not familiar, they can use the computer to get direct, real-time access to on-line legal database services, where they can gather information on the case and related precedents. Therefore mobile computers allow immediate access to a wealth of information, making people better informed and prepared.

- **IN COMPANIES**

  Managers can use mobile computers in, say, and critical presentations to major customers. They can access the latest market share information. At a small recess, they can revise the presentation to take advantage of this information. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can leverage competitive advantages.

- **STOCK INFORMATION COLLATION/CONTROL**

  In environments where access to stock is very limited ie: factory warehouses. The use of small portable electronic databases accessed via a mobile computer would be ideal.

Data collated could be directly written to a central database, via a CDPD network, which holds all stock information hence the need for transfer of data to the central computer at a later date is not necessary. This ensures that from the time that a stock count is completed, there is no inconsistency between the data input on the portable computers and the central database.

- **CREDIT CARD VERIFICATION**

  At Point of Sale (POS) terminals in shops and supermarkets, when customers use credit cards for transactions, the intercommunication required between the bank central computer and the POS terminal, in order to effect verification of the card usage, can take place quickly and securely over cellular channels using a mobile computer unit. This can speed up the transaction process and relieve congestion at the POS terminals.

- **TAXI/TRUCK DISPATCH**

  Using the idea of a centrally controlled dispatcher with several mobile units (taxis), mobile computing allows the taxis to be given full details of the dispatched job as well as allowing the taxis to communicate information about their whereabouts back to the central dispatch office. This system is also extremely useful in secure deliveries i.e.: Securicor. This allows a central computer to be able to track and receive status information from all of its mobile secure delivery vans. Again, the security and reliability properties of the CDPD system shine through.

- **ELECTRONIC MAIL/PAGING**

  Usage of a mobile unit to send and read emails is a very useful asset for any business individual, as it allows him/her to keep in touch with any colleagues as well as any urgent developments that may affect their work. Access to the Internet, using mobile computing technology, allows the individual to have vast arrays of knowledge at his/her fingertips.

  Paging is also achievable here, giving even more intercommunication capability between individuals, using a single mobile computer device.

## MOBILE DEVICE SECURITY CHALLENGES:

**PROTOCOL COVERAGE IS LACKING**: Mobile devices often rely on built-in firewalls or enterprise network isolation. The protection that firewalls provide is only as good as the policy they are configured to implement and there are a whole slew of issues related to remote security policy management of unthread devices.

I expect that analysis of network exploits on mobile devices with internal firewalls, will match analysis of real-world configuration data from corporate firewalls that shows rule sets that frequently violate well-established security guidelines (for example zone-spanning objects and lack of stealth rules).

In addition, a state-full inspection firewall on a mobile device doesn't perform deep content inspection on complete sessions and is therefore blind to data theft attacks – for example piggy-back attacks on text messaging in order to steal sensitive data.

**PROXY-BASED ACCESS TO CONTROL A DEVICE IS CONVENIENT but** may enable attackers to compromise a device and steal data – proxies' end-point devices to obtain direct access to the Internet – research with clients show us that as much as 20 percent of all endpoints already bypass content filtering proxies on the enterprise IT network.

**VISIBILITY OF NETWORK TRANSACTIONS IS USUALLY MISSING MAKING INCIDENT RESPONSE VERY DIFFICULT**: Firewall and proxy logs are generally never analyzed, and often lag hours behind an event. An IPS often relies on anomaly detection. Anomaly detection relies on network flow data, which is often reported at intervals of 15 to 45 minutes. With that kind of lag, an entire network can be brought down.

Because anomaly detection is looking for an anomalous event rather than an attack, it is frequently plagued by time-consuming false positives. A proxy on the other hand relies on URL filtering and simple keyword matching that analyzes the HTTP header and URL string. By looking at content and ignoring the network; a proxy can suffer from high rates of false negatives, missing attacks.

**MULTIPLE SECURITY AND APPLICATION LAYERS** increases cost of implementation and maintenance. Installation of multiple, disparate, proxy-based security products complicate network and end-point maintenance. Proxies require changes to the network infrastructure and in large networks may be impossible to install.

Updating mobile device application software to latest patch levels can be challenging to enforce and control and may result in injecting new software vulnerabilities into the device as there is probably not central IT administrator in charge of updating the mobile electronic medical records application running on 300 Android tablets in the hospital.

**REDUNDANT, MULTIPLE NETWORK SECURITY ELEMENTS INCREASE RISK IN THE OVERALL SOLUTION**: This is additional risk that manifests itself as a result of the interaction between mobile devices accessing cloud services via a complex system of cache servers, SSL accelerators, Load balancers, Reverse proxy servers, transparent proxies, IDS/IPS and Web Application Firewalls.

Consider that endpoints can bypass SSL proxies by specifying a gateway IP address and transparent proxies on a Windows network are no assurance for unauthenticated user agents bypassing the entire proxy infrastructure. HTTP-Aware firewalls such as Web application firewalls can be completely or partially bypassed in some cases.

Transparent proxies can be compromised by techniques of HTTP response splitting since they rely on fine-grained mechanisms of matching strings in HTTP headers. This is why Mozilla is delaying their implementation of Web sockets which may not matter if you're running Chrome OS.

## ARCHITECTURE OF MOBILE COMPUTING/ CELLULAR NETWORK:

A mobile/cellular network consists of mobile units linked together to switching equipment, which interconnect the different parts of the network and allow access to the fixed Public Switched Telephone Network (PSTN). The technology is hidden from view; it's incorporated in a number of transceivers called Base Stations (BS). Every BS is located at a strategically selected place and covers a given area or **cell** - hence the name cellular communications. A number of adjacent cells grouped together form an **area** and the corresponding BSs communicate through a so called Mobile Switching Centre (MSC). The MSC is the heart of a cellular radio system. It is responsible for **routing**, or **switching**, calls from the originator to the destinator. It can be thought of managing the cell, being responsible for set-up, routing control and termination of the call, for management of inter-MSC hand over and supplementary services, and for collecting charging and accounting information. The MSC may be connected to other MSCs on the same network or to the PSTN.

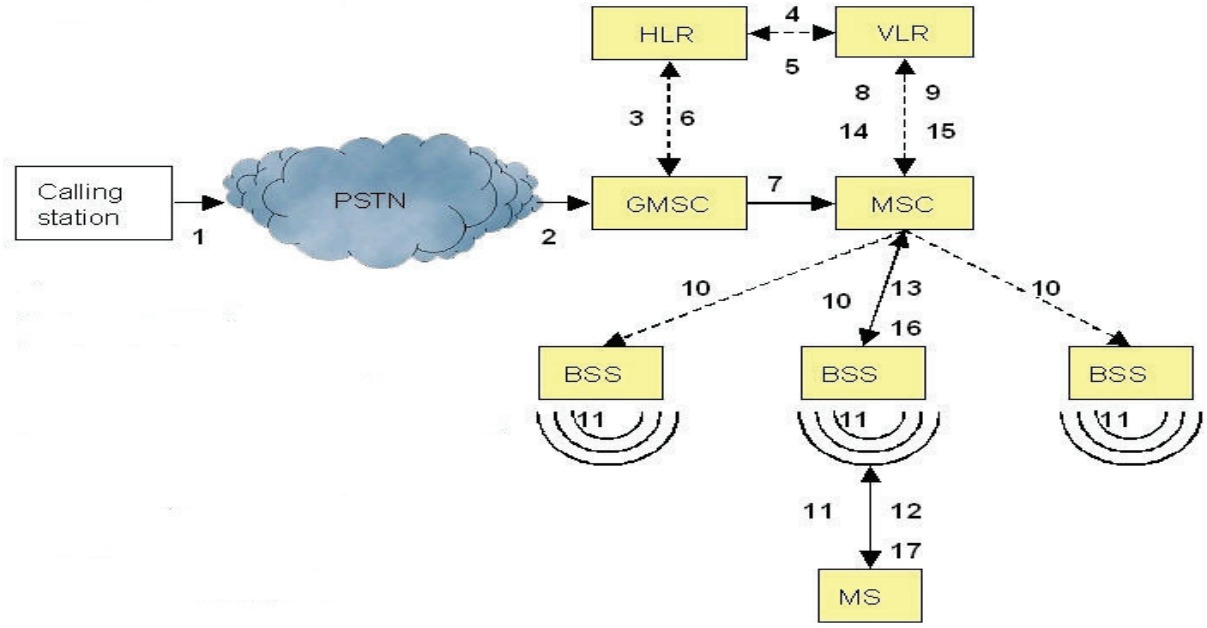



**Figure: Mobile Switching Centre**

## Process of above figure:

1: Calling a GSM subscriber
2: Forwarding call to GMSC
3: Signal call setup to HLR
4, 5: Request MSRN from VLR
6: Forward responsible MSC to GMSC
7: Forward call to current MSC
8, 9: Get current status of MS
10, 11: Paging of MS
12, 13: MS answers
14, 15: Security checks
16, 17: Set up connection