B.TECH.

EIT-505

FIFTH SEMESTER EXAMINATION 2010-11

INFORMATION SECURITY AND CYBER LAWS

1. Attempt any four parts: (4 × 3 = 12)

Q.1 (a) What are Information systems? Explain how distributed Information system help global organizations?

Ans. An Information system is a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision-making and control in an organization. Information system may be defined as organized collection of human, software, hardware and communication equipment and database, in which the person controls, process and communicate the information.

The overall objective of the information system is to gather the data, processing the data, communicating the information to the user of the system. Thus Information System accepts data from their environment and manipulates the data to produce information that is used to solve a problem or address a business need.

The information systems of today are distributed and component based. IS used by business enterprises are no more monolithic and no more are the housed in a single location. The term extended enterprise resulting from a new way of doing the business, namely the electronic business or e-business. So, prior to e-business days, not only the suppliers and consumers remain separated but the knowledge/procedure workers and business personnel also remained relatively unconnected. It required distributed computing. The extended enterprise serve the needs of networked enterprises, the information system are no more confined to a single location, single computer that is a distributed system.

Q.1. (b) What are decision support system? Discuss major functional requirement of a decision support system.

Ans. A decision support system is a collection of software and hardware to support decision-making in specific environment or problem. DSS supports management solving business problems DSS (Decision support system).

Are often designed as per manager's requirement and plays a vital role in making managerial 'judgments'. Decision support systems (DSS) are designed around business policies and methods for decision-making.

Q.1. (c) What are security threats in mobile computing. Explain how are they dealt?

Ans. Mobility brings two main challenges to the information system's security, on the handheld devices information is taken outside the physical controlled environment and controlled environment and remote access back to the protected environment is granted. Perceptions of the organizations to these security challenges are important in devising appropriate security operating procedure.

Some of the well known technical challenges in mobile security are:

(a) Managing the registry settings and configurations.

(b) Authentication service security.

(c) Cryptography security

(d) Light weight directory access protocol (LDAP) security.

(e) Remote access server (RAS) security.

(f) Media player control security

(g) Networking application program interface (API) security, etc.

The organizations needs to establish security practices at a level appropriate to their security objectives, some organizations will implement security procedures and tools extensively, while others will place more value on cost and convenience.

- The best security technology features are worthless if there is no organization policy or automated enforcement.
- Tracks should be maintained of who owns what kind of mobile devices.
- Mobile devices of employees should be registered in corporate asset register.
- Remove logical as well as physical access to corporate resources on leaving of an employee.

Q.1. (d) What do you mean by Information security? Distinguish between information level threats and Network level threats.

Ans. Given the crucial role played by information system, it is important that they remain secured and that the data contained in them do not fall into the hands of those who are not intended to have access to it. Security of information systems becomes particularly important with the advent of internet. The access by internet allows a mass of information to remain up to-date in real time, but it also opens the door for external encroachment. Thus information security deals with the process of securing your information system from external as well as internal attacks.

It is important to distinguish 'information level threats' from 'network level threats'. By network based threats we mean that in order to become effective, potential attackers require network access to corporate computer systems or to networks used by corporate computer systems. Example for network based threats are hacking of computer system and launching of DoS attack as well as spreading malicious code such as viruses.

Information level threats also use heavy use of network but at the primary level is the content of a message and not its form. Sending fake enquiries to service accounts to eat up resources. (e.g. flooding the mail server with many messages so that it gets choked.) would qualify as an information based attack.

Q.1. (e) What do you mean by RFID? How RFID can be used in mobile commerce and Information asset protection?

Ans. With Radio frequency identification technology, both the electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver, which read the RF and transfer the information to a processing device, and a transponder or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted. With RFID tag, you can track your stolen/ lost laptop.

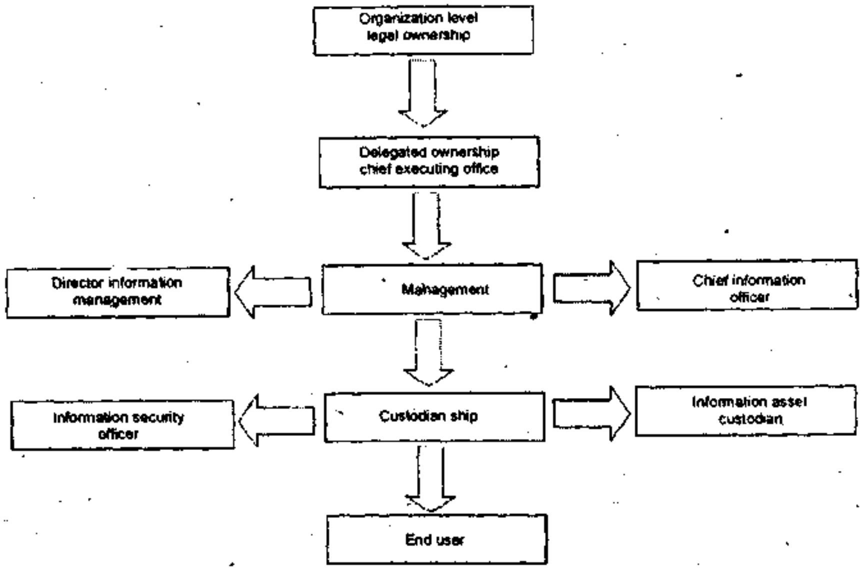
RFID systems can be used just about anywhere, from clothing tags to missiles to pet tags to food, anywhere that a unique identification is needed. The tag can carry information as simple as a pet owner's name and address or the cleaning instruction on a sweater to as complex instructions as on how to assemble a car. Some auto manufacturers use RFID systems to move car through an assembly line.

- One key difference between barcode and RFID is that the RFID eliminates the need for line of sight reading something that bar coding depends on.
- RFID reading can be done at greater distances than bar coding scanning.
- RFID is also dedicated short range communication (DSRC.).

Q.1. (f) Explain different roles involved in managing information as 'asset'. How does the role of custodian differ from the role of user?

Ans. The different roles involved in managing information as asset are given below:

1. Legal owner
2. Chief executive officer
3. Management
4. Custodian
5. End user


Organization level legal ownership
Delegated ownership chief executing office
Director information management
Mahagement
Chief information officer
Information security officer
Custodian ship
Information asset custodian
End user

Custodian Roles and Responsibilities:

- Develop policies, procedures and standards to ensure the security, confidentiality and privacy of information.
- Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
- To ensure that information asset have been assigned appropriate security classification.
- Maintenance and upkeep of asset.
- System recovery
- Backup of the information
- Updating of information asset inventory register.
- Whereas, end users are authorized by the custodians to access information and use safeguards established by the custodian.
- The users are bound by the acceptable usage policy of the organization.

2. Attempt any four parts: (4 × 3 = 12)

Q.2. (a) What do you mean by electronic commerce? What are benefits of electronic commerce for business firms? What precautions must be taken to ensure confidentiality of the document sent over the network?

Ans. Electronic commerce or e-commerce is the process of buying and selling or exchanging of products, services and information through electronic media. Example - online shopping, net banking.

Types of E-Commerce:

1. **B2B e-commerce:** B2B (Business to Business) involves online transaction between two or more business organization. In B2B the companies buying and selling of the product and services to each other.
2. **B2C e-commerce:** In B2C (Business to Consumer) the companies that sells the products and services to customers online. It provides a direct sale between the supplier and individual customer.

3. **C2B e-commerce:** The transaction originated by the customer has a set of requirement specifications and specific price for a commodity, service or item.
4. **C2C e-commerce:** C2C (Consumer to Consumer) is defined as exchange of products between consumers.

Benefits of e-commerce for business firms:

1. Increased potential market share.
2. Low-cost advertising
3. Low-barriers to entries
4. Strategic benefit: it helps reduce the delivery time, labor cost and cost incurred in the following are:
   - Document preparation
   - Error detection and correction
   - Telephone calling
   - Data entry
   - Overtime

Precautions to ensure confidentiality of the document sent over internet:

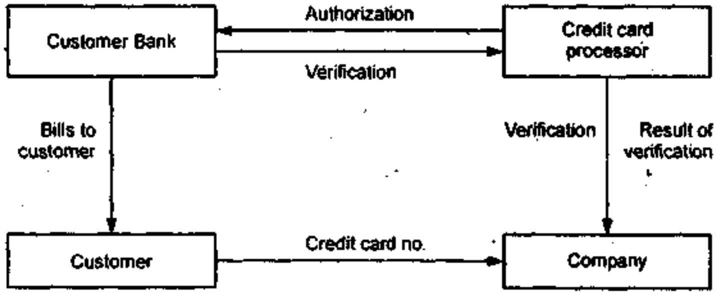
- Be aware of the enemy
- Work with a limited number of secrets
- User education is always critical
- User awareness and training on security
- Avoidance of Lax/ lazy behavior of humans.

Q.2. (b) What do you mean by payment instruments used in electronic commerce? Explain the difference in credit and debit cards.

Ans. Payment Instruments used in e-commerce: The payment instruments are the methods of making the payment for the product and money exchange. The popular payment instruments being used in e-commerce are as follows:

Electronic Cash: The payment instrument known as digital cash or e-cash, allows person to pay for goods or services by transmitting a number from his computer subsystem to the merchant computer system. One of the key features of digital cash is that it's anonymous and reusable, just like real cash.

Credit/Debit card: Credit cards are issued by financial institutions which allow making a purchase up to a certain limit or credit. Most of the credit card companies recognize the organization or shops etc. from where the items are purchased. Payments of these items are paid by the credit card company on user's behalf. They regularly send bills to the customers for shopping they have done.



Debit cards on other hand are issued by the financial institutions/ banks in which user have their accounts. Debit cards allow making a purchase up to the limit of balance in the account of the holder. That is the amount of shopping done is debited from the account of the holder and if the amount of shopping is more than the balance present in account than the transaction is declined and does not complete. This is the only difference between credit and debit cards.

Q.2. (c) What do you mean by access control to an information resource? Discuss difference in authentication and user identification.

Ans. Access control refers to the rules and deployment mechanisms that control access to information security, and physical access to premises. The entire subject of information security is based on access control, without which information security cannot be defined.

Access control to an information resource deals with the following:

- Is there any perimeter control for protecting against access? Is it regularly monitored or tested?
- Is the resource secure against penetration by intruders' bomb, gun or arson attack?
- Is access to the resource restricted to only those who have authorized access?

Authentication: This is the testing or reconciliation of evidence of a user's ID. It establishes the user's ID and ensures that the users are who they say they are: Authentication is a security measure designed to establish the validity of a transmission, message or originator or a means of verifying on individual's eligibility to receive specific categories of information.

Identification: It indicates the mean by which user claims their identities to a system. It is most commonly used for access control, and is necessary for authentication and authorization.

Q.2. (d) What do you mean by biometric data? Discuss the advantages of biometrics over traditional authentication methods.

Ans. The term biometrics comes from a Greek word Bios meaning life and Metrikos meaning measure.

- It is well known that the human intuitively uses somebody characteristics such as face, voice etc. to recognize each other.
- Biometrics is used as one of the methc d for physical access control.
- Biometric is a collection of method fc r identification based on measuring tim e physiological characteristics that are unique to each and every individual.
- Dome examples of such characteristics are:
  1. Voice
  2. Finger prints
  3. Boy contour
  4. Retina
  5. Hand writing style

Biometrics data have characteristics which are so unique to a person and embedded with a person that it cannot be lost, stolen and copied. Given the unique nature of human biometrics ID, biometrics methods occupy an important place in user identification/authentication.

Advantages of Biometrics: Traditionally passwords and ID cards have been used to restrict access to secure system but these methods can easily be breached and are unreliable.

- Biometric cannot be borrowed, stolen or forgotten and forging one is practically impossible.
- From the preceding discussion, one can see that biometric is an alternative to using passwords for authentication in logical control.
- Biometric is based on the third type of authentication mechanism.
- Biometric is defined as automated means of identifying or authenticating the ID of a living person based on physiological or behavioral characteristic.
- In biometric, identification is a 'one- to-many' search of an individual characteristic from the database of stored image.
- Biometric provide a number of benefits compared to the traditional method.

1. Increase thè level of security
2. Greater convenience
3. Higher level of accountability
4. Fraud detection.

Q.2. (e) What do you mean by physical security for information systems? What physical security measures are generally used for typical information system resources?

Ans. Physical Security protects the facilities housing system resource, the system resource themselves and the facilities used to support their operation. Physical Security, as it pertains to computer security, should cover the following area at a minimum: access control, fire safety, and failure of supporting utilities, structural collapse and portable system.

Physical security measures:

1. Security keys and containers to protect classified information.
2. Physical access control measures.
3. Security alarm system to detect unauthorized access.
4. Physical barriers to deter detect and delay unauthorized entry.
5. Continuous surveillance over secure areas.

Q.2. (f) What are legal challenges in deployment of biometric in public domain applications?

Ans. Legal issue, the purpose for which information about individuals is collected and how it can be then used the ability to access information and redress inaccuracies and providing robust security so that persons cannot have their information compromised.

The following four themes describe the legal challenges of biometrics:

1. **Enabling legal environment:** The existing legal environment (privacy and data protection) is flexible in that it is an enabling legislation legitimizing the facto commercial use of personal data. Data protection rules regulate the use of biometrics but they lack normative content and ethical debate.
2. **Opacity/ transparency rules required:** Data protection (transparency rules) does not specify what the limits of use and abuse of biometrics are opacity (privacy) rules may prohibit use in cases where there is the need to guarantee against outside steering.
3. **Fundamental concerns arising with wider applications:** A biometrics is diffused in society, some concerns are gaining in importance - concerns about power accumulation further use of existing data specific threats related to use of biometric by the public sector and the failure to protect individuals from their inclination to trade their own privacy within what seems to be very low cost convenience.
4. **Use of biometrics in law enforcement:** It is imperative that biometrics evidence be regulated when presented evidence in courts of law so as to protect suspects adequately.

3. Attempt any four parts: (4 × 3 = 12)

Q.3. (a) What are electronic payment systems? Compare electronic payment system on internet with conventionel payment mechanisms.

Ans. Electronic payment are the central part of e-commerce activities as it deals with the strategies for the payments of goods and services by online customers. Electronic payment system implies cryptography. The original purpose of cryptography was to hide something that had been written.

- Cryptography can be used to hide the meaning of information in any form, such as data stored on a disk or message in transit through a communication network.
- When electronic payments are sent through a network the biggest risk is that payment message might be altered and

the risk that someone reads the message may be of a minor significance.

- The process of checking the integrity of the transmitted message is often called message authentication. The most recent and useful development in the uses of cryptography is the digital signature.
- It can prevent fraud in electronic commerce and assure the validity of financial transaction.

Conventional instruments of payments such as demand drafts, credit notes, checks are not suited to e-commerce. Conventional instruments are too slow to be processed and the overheads in processing such instruments may be high. Various instruments which may be used to make payment on the internet are credit/debit cards, smart cards, e-cash, electronic wallet etc. Important issues related to the electronic payments system are, how to minimize the financial risk such as leakage of information, mistakes and frauds and finally devising methods for the completion of electronic payment cycle.

Several protocols have been devised and deployed to provide the necessary security to payment transactions. Some protocols are as follows:

1. Secure electronic payment protocol (SEPP)
2. Secure electronic transaction protocol (SET)

Q.3. (b) List broad activities involved in settlement of a business transaction in e-commerce. List issues related to safety of business transaction on web.

Ans. A business transaction on web involves mainly three activities:

1. Search of product
2. Price negotiation
3. Delivery of products and payments

There are several ways of making payments on the internet using credit and debit cards. This is electronic currency since payment has to travel on the network from one computer to another computer, so many internet security breaches occurs.

Inspite, of these cases most customers, banks, researchers are of the view that e-commerce transactions are far safer than those in the physical world with the newer versions of web browsers like Netscape navigator and MS Internet explorer, transactions can be encrypted using secure socket layer.

All credit card companies are promoting an additional security standard called secure electronic transactions. This standard encodes the credit card numbers in such a way that it can be decoded only by their bankers and credit card companies. The security of electronic fund transfer or electronic payment transaction is intimately related to model of encryption used for encrypting it. Therefore, electronic transactions are for safer than what is generally imagined.

Q.3. (c) What are objective, requirement and threats in a cryptographic system? What do you mean by Non-repudiation in such systems? Discuss the issue of integrity and authentication of the documents.

Ans. Objective: the original purpose of cryptography was to hide something that had been written. Thus, cryptography is used to hide the meaning of information in any form. Such as data stored on a disc or a message in transit through a communication network. Cryptography can be applied to anything that can be digitally coded such as: Software, graphics or voice.

Requirement: From e-mail to cellular communication from secure web access to digital cash, cryptography is an essential part of information system. It helps provide accountability, fairness, accuracy and confidentiality. It can prevent fraud in e-commerce and assure the validity of financial transactions. It can be used to protect one's anonymity.

Threats: The threats to a cryptographic system are as follows:

1. Brute force attack (breaking the key)

2. Password hacking
3. Packet sniffing
4. Modification of the original document.

Non Repudiation: It is the method by which the sender of the message/ data is provided with a proof of the delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Integrity: The concept of integrity ensures that:

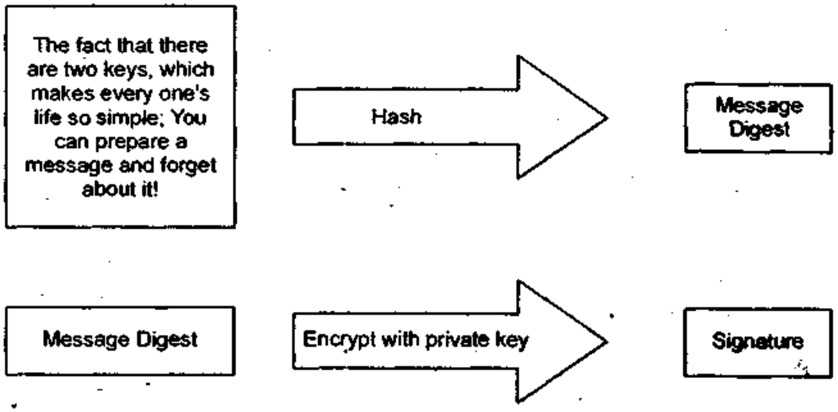
1. Modifications are not made to data by unauthorized personnel or processes.
2. Unauthorized modifications are not made to data by authorized personnel or processes.
3. The data are internally and externally consistent.

Authentication of Documents: This is the testing or reconciliation of evidence of document's ID. It establishes a document id and ensures that documents/ programs are those they say they are. It is a security measure designed to establish the validity of the transmission, message or originator or a means of verifying a document/ program's eligibility to do specific tasks.

Q.3. (d) What is digital signature? How digital signatures are related to public key cryptographic systems?

Ans. With private key and right software, a user can put digital signatures on documents and other data. A digital signature is a 'stamp' user places on the data that is unique to him/her and is very difficult to forge. In addition, the signature assures that any changes made to the data that have been signed cannot go undetected.

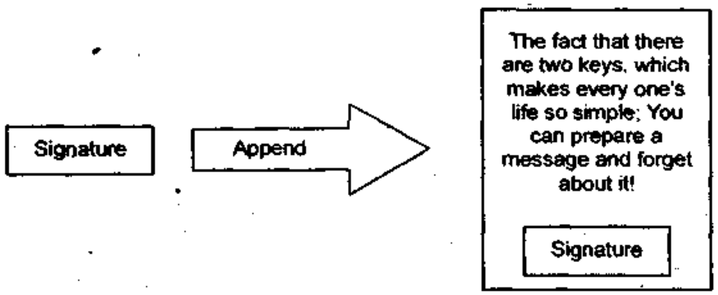
To sign a document, a person using the keys will use suitable software available to crunch down the data into just a few lines by a process called **'hashing'**.


The fact that there are two keys, which makes every one's life so simple; You can prepare a message and forget about it!
Hash
Message Digest
Message Digest
Encrypt with private key
Signature

Message Digest: A message digest is a product of a one way hash function applied on a message; it is a fingerprint or a unique summary that can uniquely identify the message. However, it is not possible to change a message digest back into the original data from which it was created.

The software then encrypts the message digest with the private key. The result is the digital signature.

Finally, the software appends the digital signature to the document. All of the data that were hashed have been signed.

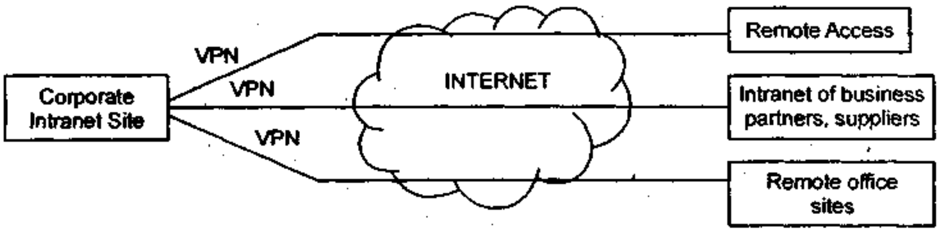

Signature
Append
The fact that there are two keys, which makes every one's life so simple; You can prepare a message and forget about it!
Signature

Digital signatures are related to public key cryptography as:

- It allows the recipient of the information to verify that it has not been modified in transit.

Q.3. (e) What do you mean by virtual private networks? Discuss authentication mechanism used in a virtual private network.

Ans. Virtual private network (VPN) is a network of virtual circuits that carries private traffic through public or shared networks such as the internet or those provided by network service providers. VPNs allow a trusted network to communicate with another trusted network over un-trusted / public network such as internet. VPNs are used primarily to extend an enterprise's internal private network (intranet) across un-trusted public networks. They provide the capability to securely convey information across the public network into the corporate network.



VPN

Authentication Mechanism: A VPN involves two entities: the protected or 'inside' network, which provides physical and administrative security to protect the transmission, and a less trustworthy, that is 'untrusted' outside network or segment. A firewall sits between remote user's workstation or client and the host network or server. As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter.

For better security, many VPN client programs can be configured to require that, all IP traffic must pass through the tunnel while the VPN is active with an organization's internal networks that is protected from the outside internet by a firewall, people who share it may be simultaneously working for different employers over their respective VPN connections from the shared internal network. Each employer would therefore want to ensure that their proprietary data are kept safe and secure even if another computer in local gets infected with malware.

4. **Write short notes on any 2 of the following: (2 × 7 = 14)**

Q.4. (a) Intellectual property Rights

Ans. (i) IPR laws: IPR stands for intellectual property right, which can be defined as rights acquired over a property created with the intellectual effort of an individual.

The property is intangible in nature. IPR is divided into 7 main branches under the TRIP (Trade related aspects of IPR) agreement. These branches are:

1. Patents
2. Copyright
3. Trade marks
4. Geographical indication
5. Layout design for IC
6. Design registration
7. Confidential information

(ii) Patent law: Patent law protects the 'device or process' for carrying out an idea; the two critical requirements are - 'the device or process' works in a new and inventive way and that is capable of industrial application. The economic justification for patent law is to encourage inventors, by creating an artificial monopoly for the exploitation of the inventions. Generally patents need to be registered with a central authority.

The patent owners have the exclusive right to make use, or sell the inventions.

(iii) Copyright law: Copyright is a legal concept that gives the creator of original work exclusive rights to it, usually for a limited period of time. In its most general form, it is literally 'the right to copy', but also gives the copyright holder the right to be credited for the work.

In short it gives exclusive right to copy, adopt, distribute and perform that material. However, unlike patent law, the right is not 'exclusive'; therefore, copyright in a work can exist with two different people if it can be proved that each version of the work was developed independently.

There are four main forms of remedies in the event that copyright infringements take place:

1. An injunction to stop the production of further copies.
2. A demand that all copies are surrendered to the copyright owner.
3. Damages for losses suffered by the copyright owner.
4. An account of profits made by the infringer.

(iv) Trademarks: Trademarks may be words or symbols, identifying the origin or ownership of a particular merchandise or product to which it is applied. By registering a trademark, the owner legally reserves the exclusive use of trademarks.

(v) Geographical indications: Geographical indications of goods are defined as the aspect of industrial property, which refers to the geographical indications referring to a country or to place situated there in as being the country or place of origin of that product.

(vi) Design Registration: are used to protect products distinguished by their novel shape or pattern. They are available for one off items.

Q.4. (b) Ethical and legal issues in data and software piracy

Ans. Date privacy issue: Data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Privacy concerns exist wherever personally identifiable information is collected and stored in digital form. Improper or nonexistent disclosure can be the root cause for private issues. Data privacy issue can arise in response to information from a wide range of sources such as:

- Health Care records
- Financial Institutions and transactions
- Residence and geographic records
- Organizational records
- Ethnicity

The challenge in data privacy is to share data while protecting personally identifiable information.

Software privacy issue: Software has the ability to store vast amount of information about individuals. Software can be designed to recognize faces, monitor, e-mail, analyze consumer spending habits, track web surfing and record other pattern and activities. Information tracking software has raised much privacy concern.

Consumer privacy concern: Consumer can have their purchasing habit closely tracked. Web surfing habits are also tracked by corporations to prevent piracy.

Business monitoring employers: Businesses use software to read their employee's email and in some cases employ staff to employee email. Additional, certain words used in emails will activate software's that notifies third parties of email containing those words.

Government software and privacy rights: Law makers have expressed concern over government softwares that allow military, intelligence and law enforcement agencies to recognize pattern indicative of terrorism or criminal activity in personal data and web surfing.

Hackers: They are the people who specialize in unauthorized access of private information stored in computers. Hackers cab share information and techniques that allow them to violate an individual or organization's privacy and security. Hackers are a big concern to law enforcement and the private sector.

Q.4. (c) Types of Cyber Crimes.

Ans. "Cyber Crime" can be said to be an act of omission, committed on the internet, whether directly or indirectly, which is prohibited by any law for which punishment is provided. In simple language we can say that the unlawful activity (crime) done in which computer/ internet has played any role, is known as Cyber Crime.

Cyber crime can be classified as, Old crimes, committed on or through the new medium of the internet. For example fraud, defamation, harassment, pornography, threats etc.

Types of threats related to cyber crime include:

1. **Spreading Computer Viruses:** Segments of code that is able to perform malicious acts. Viruses disrupt the normal working of a program, software or a computer. A computer virus can be spread using any of the following mediums:
   - E-mails
   - Multimedia (Songs, movies etc.)
   - Internet
   - Removable disks (CD, Pen drives etc.)
2. **E-mail Spoofing:** Using someone else's e-mail ID to send e-mails. However, the e-mail in reality has not been sent from that ID which it tends to be coming from. The e-mail Id has only been spoofed. i.e. Fake e-mails. Example: You send an email to your friend, which tends to be coming from Bill Gates ID (billgates@microsoft.com), it says "Microsoft wants to hire you". Thus, the mail in reality has not come from Bill Gates Id. This is known as email spoofing.
3. **Hacking:** Out of all Cyber crimes, Hacking is amongst the biggest threats to internet and e-commerce. Hacking refers to breaking into computer systems without permission and stealing important or valuable information. An act which comprises of viewing, sharing, modifying or stealing someone's data/files without his/ her permission is termed as hacking.

4. **DoS Attack:** Denial of Service (DoS) attack is used to attack the target system/server with large no. of requests, which it cannot handle and ultimately crashes. It means sending large number of requests to a system generally higher to the capacity which it can handle. DoS attack is generally used by hackers to break down a web site or to affect its normal working. Recently, Face book and Google, both were the victims of Denial of Service attack and bear a loss worth millions of dollars.
5. **E-mail Bombing:** Sending large number of e-mails to a particular ID/person. i.e. bombing his/her inbox with hundreds or thousands of e-mails together. It sometimes results in crashing the inbox.