B.Tech. EEC-505

SIXTH SEMESTER EXAMINATION, 2010-11

INFORMATION SECURITY AND CYBER LAWS

Time: 3 *Hours* *Total Marks:* 100

Note: *Attempt all questions.*

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

Q.1. (*a*) What is Information System? Describe the need of distributed information system.

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 is the difference between security and threats and explain the web security?

Ans. Security: 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.

Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity.

Threats: A threat is a possible event that can harm an information system.

Security threats have four principal sources:-

1. **Human error:** for example, inadvertent disclosure of confidential information.
2. **Computer abuse or crime:** A generic example is when a person intends to be malicious and starts to steal information from sites, or cause damage to, a computer or a computer network.
3. **Natural and political disasters:** This can happen in the form of natural calamities and wars, riots etc.
4. **Failure of hardware or software:** for example, server malfunctioning, software errors etc.

Security threats related to computer crime or abuse include:

1. Impersonation
2. Trojan horse method
3. Logic bomb
4. Computer viruses
5. DoS etc.

Web Security: addresses security when data is exchanged as part of a Web service.

Web-Security specifies enhancements to SOAP (Simple Object Access Protocol) messaging aimed

at protecting the integrity and confidentiality of a message and authenticating the sender. Web-Security also specifies how to associate a security token with a message, without specifying what kind of token is to be used. Thus, Web security deals with the security of the services provided on and by the web. It generally deals with the security of the Web site and Web services.

Q.1. (c) Explain how confidentiality can be achieved? Also describe "Integrity", "Availability" in Information security.

Ans. The following three concepts are considered the pillars of information security: Confidentiality, Integrity and Availability (CIA). These concepts represent fundamental principles of information security. All the information security controls and safeguards, and all the threats, vulnerabilities and security processes are subject to this CIA yardstick.

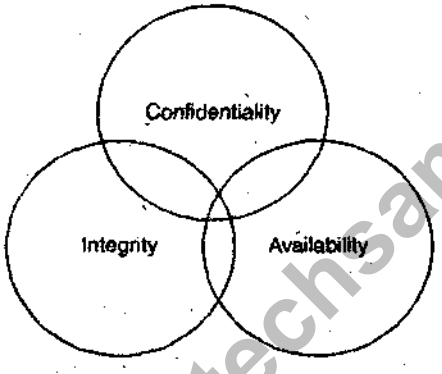


Fig. 1.

Confidentiality: The concept of confidentiality implies an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights.

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, i.e. the internal information is consistent among all sub entities and the internal information is consistent with the real world, external situation.

Availability: The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. Availability guarantees that the systems are up and running when they are needed and the security service needed by security practitioner are in working order.

Q.1. (d) Explain java applet security model. Can Java applet be harmful for the computers?

Ans. Java is designed so that programs can be dynamically loaded over the network and run locally. This very powerful paradigm promises to change the face of computing as we know it. A browser that can interpret Java byte code (such as Netscape Navigator or Internet Explorer) can download and locally execute applets that are embedded in a Web page. This activity of downloading and executing is completely automatic, requires no user approval, and sometimes occurs without the user even knowing. Remember, by simply pointing your browser at a Web page containing an applet, you start Java. Any applet started in this fashion is not required to advertise its presence. More and more Java applets appear on the Web every day. Applets are becoming ubiquitous. This means that surfing the Web with a Java-enabled browser is a more risky activity than surfing the Web in the days before Java.

It is extremely unlikely that all users of Java-enabled browsers will consider the security implications of surfing a site before each Web page access. If the mobile code paradigm is going to work, security concerns should be addressed in the language of the content itself. That way, users will not need to worry too much about security. Java's designers took this task to heart. One of their fundamental concerns was making the use of Java transparent, automatic, and above all, safe. As a result, Java was developed with key security issues in mind.

The original Java security model implements a sandbox that imposes strict controls on what certain kinds of Java programs can and cannot do. To the extent that the sandbox works, it allows a user to run untrusted code safely. An alternative approach to handling mobile code is to run only code that is trusted.

Java applets can do some annoying things; and it can thus harm your computer. Applets that inflict real damage on your system are almost unheard-of. When such applets do appear, it's because the security manager in a web browser or applet viewer is flawed. Java applets can install viruses from Internet through your web browser without your confirmation. Thus, it can only harm your system/computer if you allow it to download something from the third party.

Q.1. (*e*) What are the various types of data resources and network resources in information system? Give example to illustrate your answer.

Ans. Data Resource is a component of information technology infrastructure that represents all the data available to an organization, whether they are automated or non-automated. Different business organizations may have different needs. The data resource encompasses all its representation of each and every single data available to an organization. This means that even those non-automated data such as bulks of paper files in individual desks of each staff, confidential paper data hidden in steel cabinets, sales receipts, invoices and all other transaction paper documents constitute the Data Resource.

Thus, data resources must be managed effectively to benefit all end users in an organization. The data resources of information system are organized into:

Databases: A collection of logically related records of files. A database consolidates many records previously stored in a separate file so that a common pool of data record serves many applications.

Knowledge bases: Which hold knowledge in a variety of forms such as facts and rules of inference about various subjects.

Network Resources: Telecommunication networks like internet, intranet, extranet have become essential to the successful electronic business and commerce operations of all types of organizations and their computer based information system. The concept of network resources emphasizes that communication network are a fundamental resource component of all information system. Network resources include.

Communication media: Twisted pair wire, co-axial cabe, fiber-optic cable, and microwave, cellular and satellte wireless systems.

Network support: people, hardware, software and data resources that directly supports the operation and use of a communication network.

Q.1. (*f*) What is the classification of threats and describe the role of web services?

Ans. Threats consist of the following properties:

1. **Asset:** Asset is something of value to the crganization (information in electronic or pysical form, Information system, a group of pople with unique expertise, etc.)
2. **Actor:** Who or what may violate the security requirements- Confidentiality, integrity and avilability (CIA) - of an asset. Actors can be fron inside or outside the organization.
3. **Motive:** indication of whether the actor's intetions are deliberate or accidental.
4. **Access:** how the asset will be accessed by the acto (network access or physical access.)
5. **Outome:** The immediate result of violating the secury requirements of an asset (disclosure, modification, destruction, loss, interruption, etc.)

The mjor categories of damages resulting from threats to te information system are:

(*a*) Destrution of information and/or other resource.

(*b*) Corruptin or modification of information

(*c*) Theft, reroval of loss of information

(*d*) Disclosureof information (Confidential data)

(*e*) Modificatin of important and/or sensitive information

(*f*) Interruption c access to important information, software, appcations or services.

Generic Threat Profile: There are five categories of logica and physical assets:-

1. **Information:** Dcumented (paper or electronic) data or intellectul property used to meet the mission of an orgnization.
2. **Software:** Softwai applications and services that process, store r transmit information.
3. **Hardware:** IT physicl devices considering their replacement osts.

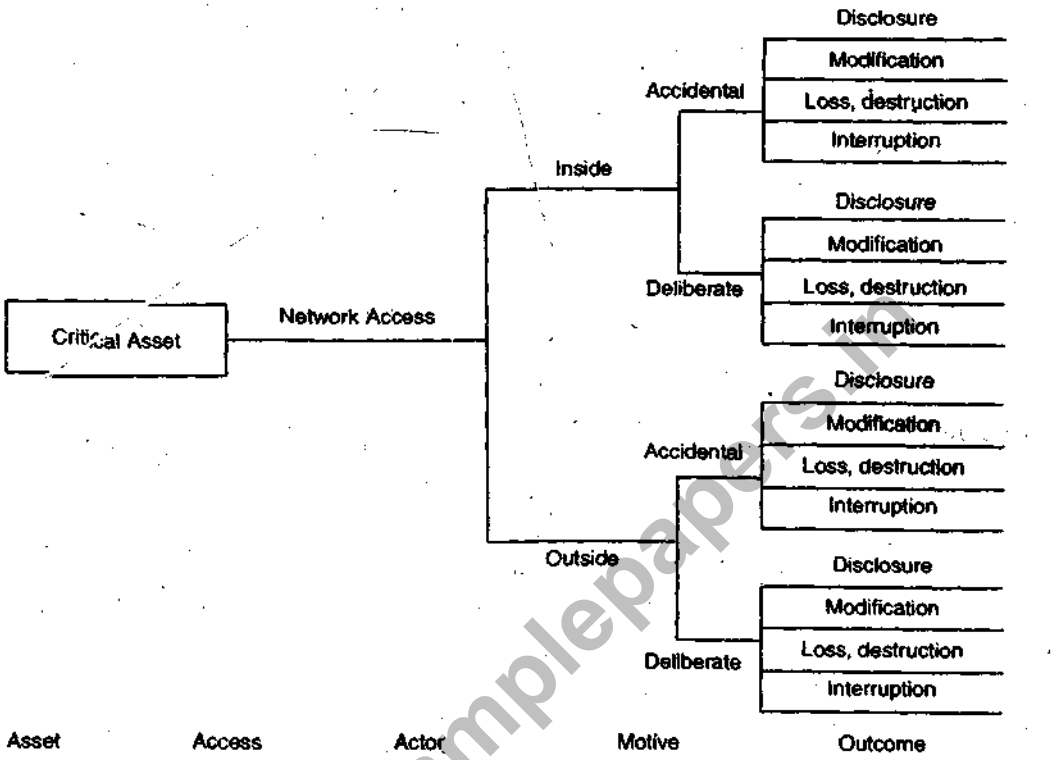


Fig. 2.

4. **People:** People in an organization who possess skills, competencies, knowledge and experience that are difficult to replace.
5. **Systems:** Information system that process and store information (a system is a combination of information, software and hardware assets.)

Another way of grouping threats is based on some common themes as follows:

1. **Human actors using network access:** The threats in this category are network-based threats to an organization's critical assets.
2. **Human actors using physical access:** The threats in this category are physical threats to an organization's critical assets.
3. **System problems:** The threats in this category are problem with an organization's IT systems. Examples include hardware defects, software defects, viruses and other system related problems.
4. **Other problems:** The threats in this category are problems or situations that are outside the control of an organization. Examples include natural disasters, power outages etc.

Role of Web Services: The internet has revolutionized communication and thereby its contribution to information sharing. With access to a computer and an appropriate connection, anyone can interact with others worldwide. Web services play a complementary and dominant role in building global information system for today's dynamic business world.

"Web services are self-contained modular, applications that can be described, published, located and invoked over a network, generally the World Wide Web (WWW)."

Web services have been proven to give a strong return on investment (ROI) and make computer based information system more adaptable. They also bring productivity, flexibiljty and low maintenance cost in the development of information system by integrating components from various third-party vendors.

2. Attempt any two parts of the following: **(6×2=12)**

Q.2. (*a*) What are the problems with traditional payment system as compared to electronic payment systems?

Ans. Traditional payment methods include cash, checks, and credit and debit cards.

These methods have several shortcomings:

- Checks and cash cannot be exchanged in real time
- Credit and debit card info exchanged over the phone or by email entails security risks
- Credit/debit cards do not support individual-to individual payment transactions
- Some individuals do not have access to credit cards or checking accounts because of credit history.
- The overhead of all but cash do not support low value transactions (micropayments)

In electronic commerce, the challenges of payment transactions were initially underestimated. Business via the internet and mobile telephony has so far been dominated by the methods of payment customary in traditional business. However, in light of advances in e-commerce, traditional business models are increasingly coming up against their limits.

Secure, user-friendly and low-priced innovative payment solutions are urgently required to boost internationally oriented e-commerce. Value-creating market players - from payment system providers, service providers, network operators and producers of terminals to financial institutions - pin great hopes on rapid progress with new payment systems.

Q.2. (*b*) What are the design issues in the biometric system? Explain benefits and criteria for selection of biometrics.

Ans. Biometric systems, by their very nature, are complex system with responsive decision making involved in term of physical access controls. The two most critical issues that designers of biometric system face are:

1. Storage and protection of the template.
2. Accuracy of biometric system step.

Storage and Protection of the template: Biometric systems have to scan, store/retrieve a template and match. It is important to note that depending on the design of the system, the match is to be performed in different locations. There can be three different 'modes of protection' that may be used for the template: no protection, data encryption or digital signature.

Accuracy of biometric system step: The evaluation of a biometric system has to be based on the evaluation of all components: the recognition system performance communication interface, the matching and decision and other key factors such as each to use acquisition speed and processing speed.

Criteria for selection of Biometrics: Biometric is a physical or biological feature or attribute that can be measured. It can be used as a means of providing without revealing your ID that you have a certain right or password.

- We know the critical difference is that biometric is something that is part of you, rather than something you know or can carry with you.
- Examples of physiological biometrics feature include height, weight, body odor, the shape of the hands, the pattern of veins, retina, the face and the pattern on the skin of thumb.
- Example of behavioral biometrics are voice pattern, signature and keystroke sequence.
- Most biometric applications are based on certain biometric information.
- Each of the various biometric techniques that exit has its own limitation.

Criteria for selection of Biometric Characteristics:

The Characteristics	The Meaning
1. Universality	1. All the human beings have same physical characteristics.
2. Uniqueness	2. For human, these characteristics are unique and thus constitute a distinguish feature.
3. Permanence	3. These characteristics remain 'persistent'.

4. Performance	4. The degree of accuracy of identification must be quite high before the system can be operational.
5. Acceptability	5. Application will not be successful if the public offer strong biometric.

Q.2. (c) Write short notes on:-

(*i*) B2B e-commerce

(*ii*) C2C e-commerce

(*iii*) B2C e-commerce

Ans. 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. That is business to business.

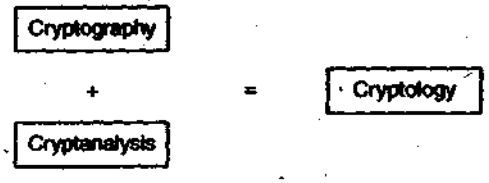
C2C e-commerce: C2C (Consumer to Consumer) is defined as exchange of products between consumers. Example- Selling and buying of second hand or old products takes place between consumer to consumer.

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. This type of e-commerce can easily be seen on the internet. There are a number of companies and Websites which do B2C e-commerce.

3. Attempt any two parts of the following: **(6×2=12)**

Q.3. (*a*) What is cryptology? Describe the difference between symmetric key cryptography and public key cryptography?

Ans. Cryptology: Cryptology is the science and art of secret communication. It is the combination of cryptography and cryptanalysis.



Symmetric key cryptography: In symmetric key cryptography same key is used for both encryption and decryption.

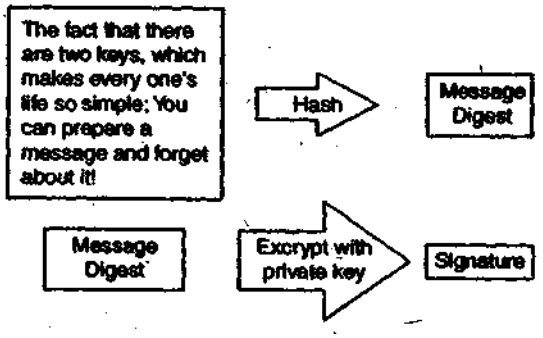
Asymmetric/Public key cryptography: In asymmetric key cryptography different key is used for both encryption and decryption.

Symmetric key cryptography	Asymmetric/Public key cryptography
Strengths: 1. Much faster than asymmetric system. 2. Hard to break with a large key size.	**Strengths:** 1. Better key distribution then symmetric system. 2. Better scalability than symmetric system. 3. Can provide authentication and non repudiation.
Weakness: 1. Requires secure delivery mechanism. 2. Key management can become overwhelming. 3. Does not provide authenticity or non-repudiation.	**Weakness:** 1. Works more slowly than symmetric key system. 2. Involves mathematical intensive tasks.

Q.3. (*b*) What are the requirements of digital signature? How authentication is maintained using digital signature?

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'**.



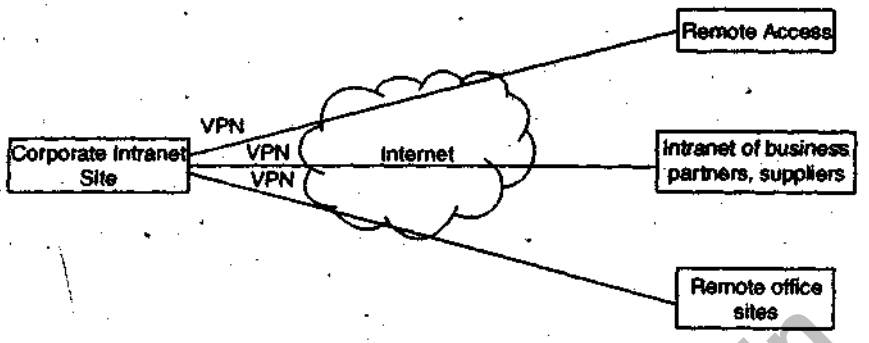
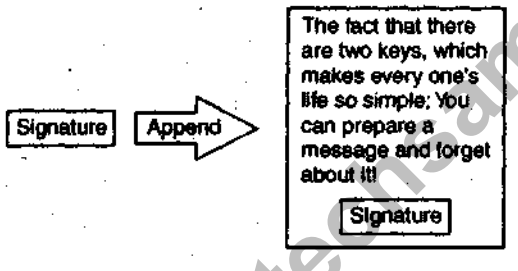


Fig. 3. VPN

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.

Maintaining Authentication - A digital signature is a message digest used to cryptographically sign a message. Digital signatures rely on asymmetric or public key cryptography. We know that to create a digital signature, you sign the message with your private key. The digital signature then becomes the part of the message. This has two effects:

1. Any changes to the message can be detected, owing to the message digest algorithm.
2. You cannot deny signing the message, because it was signed with your private key.

These two features, message integrity and non repudiation make digital signature a very useful component in message authentication.

Q.3. (c) Explain the VPN architecture and how can we implement firewall with advantages of VPN?

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.

NEED: A well designed VPN can provide great benefits:

1. Extends geographic connectivity
2. Improves security
3. Reduces operational costs versus a traditional wide area network
4. Reduce transit time and transportation cost for remote users
5. Improves productivity
6. Simplifies network topology
7. Provides global networking opportunities
8. Provides a telecommuter support
9. Provides a broadband networking compatibility
10. Provides a faster return on investment (ROI) than a traditional WAN.

VPNs have several characteristics:

- Traffic is encrypted to prevent eaves dropping
- Remote site is authenticated

- Multiple protocols are supported
- Connection is point to point

Firewalls and VPNs play a key role in securing the network against threats.

Firewalls can be relied upon to secure the networks from unwanted and unauthorized threats from the Internet. In addition, they can be used to control internal access to external resources. VPNs are used to securely connect all offices and the employees working outside the offices of the enterprise. A combination of firewalls and VPNs is used to enable authorized remote clients to gain access to sensitive information.

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

Q.4. (*a*) IPR

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*) Building Security into software life cycle.

Ans. It is important to appreciate the attention to application system's security starts right from the requirements definition stage. Secure system development lifecycle is depicted below.

1. Software requirement specification communicates the software's required performance and features to the entire team. Example- clearly starting the level of authentication for each interface [Web, command level and application program interface [API] will prevent developers from making their own assumptions about the level of trust required for the application environment.

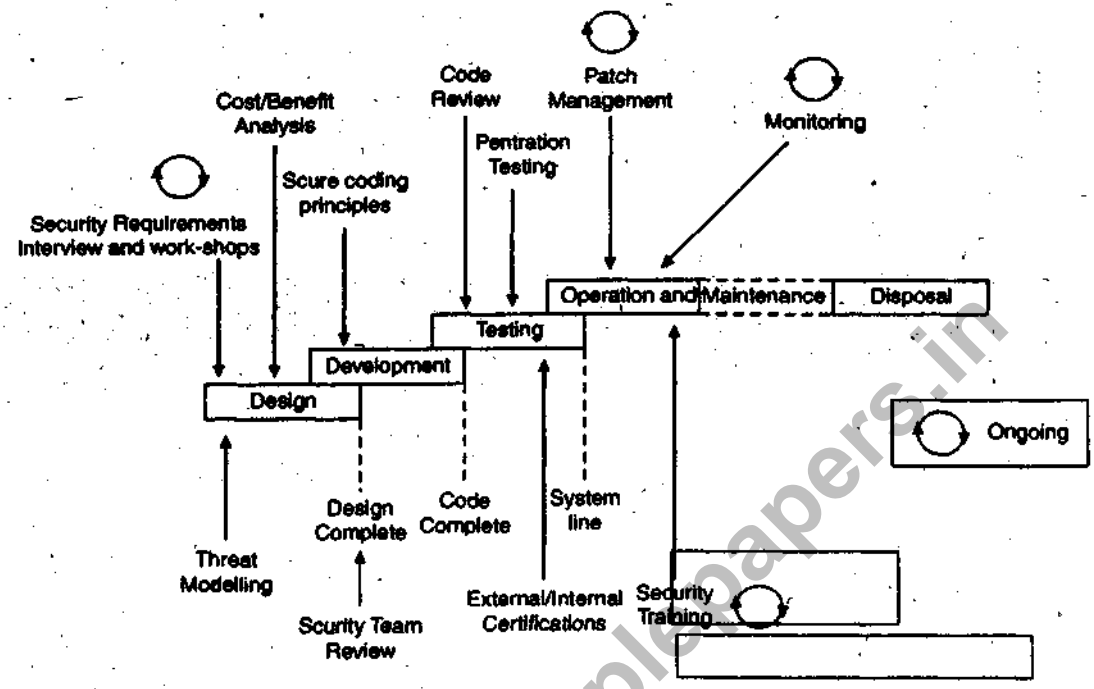


Fig. 4.

2. The next step is classifying the data- By reviewing the data that will be collected or handled by the application and assigning a classification based on their value to the organization's sensitivity and legal requirements, you can ensure security right up front.
3. The development and coding stage is, where the requirements, architecture and design come together, is critical. Developers need to understand application security threats, and must be aware of common coding errors, such as buffer overflows, injection flaws and invalidated inputs that can lead to security vulnerabilities.

Q.4. (c) 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 tq 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.