Solved Question By Hasham Malik (hawk.hasham@gmail.com)

Important topics:

Entity Relationship Diagram:

"The entity-relationship diagram (ERD) is a data model or diagram for high-level descriptions of conceptual data model, and it provides a graphical notation for representing such data models in the form of entity-relationship diagrams." E-R Diagram (E-R model) facilitates database design by allowing the specification of an “enterprise schema” which represents the overall logical structure of a database. The E-R Diagram (E-R model) is extremely useful in mapping the meanings and interactions of real-world enterprises onto a conceptual schema.

Object Oriented Analysis and Design:

The concept of object oriented analysis and design focuses on problems in terms of classes and objects. This concept combines aspects of both entity relationship diagram and data flow diagrams. The object oriented analysis and design tool has been devised to support the object oriented languages, for example C++ and Java. The roots of the concept of object orientation evolved in late 60’s with the emergence of first language “SIMULA 67” as the first object oriented language. Object oriented methodologies do not replace traditional approaches (such as data flow, process flow, and state transition diagrams); they are important new additions to the toolkit.

Centralized vs. Distributed Processing:

Centralized Processing is performed in one computer or in a cluster of coupled computers in a single location. Centralized processing was the architecture that evolved from the very first computers; however, user access was via dumb terminals that performed none of the primary processing. Today, centralized computers are still widely used, but the terminals are mostly full-featured desktop computers.

Distributed processing refers to any of a variety of computer systems that use more than one computer, or processor, to run an application. More often, however, distributed processing refers to local-area networks (LANs) designed so that a single program can run simultaneously at various sites. Most distributed processing systems contain sophisticated software that detects idle CPUs on the network and parcels out programs to utilize them. Another form of distributed processing involves distributed databases, databases in which the data is stored across two or more computer systems. The database system keeps track of where the data is so that the distributed nature of the database is not apparent to users.

Threat Identification:

“A threat is some action or event that can lead to a loss.” During this phase, various types of threats that can eventuate and result in information assets being exposed, removed either temporarily or permanently lost damaged destroyed or used for un-authorized purposes are identified.

Risk Management:

Risk Management is the process of measuring, or assessing risk and then developing strategies to manage the risk. In general, the strategies employed include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

Types of Active attacks:

Masquerading – involves carrying out unauthorized activity by impersonating a legitimate user of the system.

- Piggybacking – involves intercepting communications between the operating system and the user and modifying them or substituting new messages.
- Spoofing – A penetrator fools users into thinking they are interacting with the operating system. He duplicates logon procedure and captures pass word.
- Backdoors/trapdoors – it allows user to employ the facilities of the operating system without being subject to the normal controls.
- Trojan Horse – Users execute the program written by the penetrator. The program undertakes unauthorized activities e.g. a copy of the sensitive data.

Change management

The controlled, identification, and implementation of required changes within a computer system.

Why people resist change?

There are various reasons why people feel afraid of the change. The change may act as a favorable agent for many at the organization. However it is merely the fear of the unknown that in most cases creates hurdle.

- Fear of the unknown—mostly the reaction is "God knows what's going to happen!".
- Lack of good information – involvement from the lower levels is not taken by the management and they are not fully aware of the future happenings.
- Fear for loss of security – Mostly changes lead to downsizing which is termed mostly by organizations as right sizing.
- No reason to change – no reason sounds convincing to people to accept a change.
- Fear for the loss of power – Mostly changes make organizational structures more horizontal, flexible resulting into delegation of authority and handing over powers to lower levels.
- Lack of resources
- Bad timing – Employees sometimes are approached with a proposal of change when they are already feeling.
- Habit – people with closed mind are not innovative to learn new things and this may prove to be a major hurdle in bringing in change.

Ethical Challenges

Information system security association of USA has listed down following ethical challenges

1. Misrepresentation of certifications, skills
2. Abuse of privileges
3. Inappropriate monitoring
4. Withholding information
5. Divulging information inappropriately
6. Overstating issues
7. Conflicts of interest
8. Management / employee / client issues

Three passive attacks

Network Analysis

- Eavesdropping
- Traffic Analysis

Logical and physical attacks

Logical is from software and physical is from hardware.

Q.As a software maker make any student profile with help of flow chart ?

Q.what are the purposes of hacker?write any five?

A hacker is a person who attempts to invade the privacy of the system. In fact he attempts to gain un authorized entry to a computer system by circumventing the system's access controls. Hackers are normally skilled programmers, and have been known to crack system passwords, with quite an ease. Initially hackers used to aim at simply copying the desired information from the system. But now the trend has been to corrupt the desired information.

Q- In which type of attack, an unauthorized attacker monitors or listen the communication between two parties? Give at least one example of such type of attack.

Tapping, placement of a "bug" inside private premises to secretly record conversations, or the use of a "wired" government informant to record conversations that occur within the informant's earshot

Q-Identify any two firewall philosophies that are generally followed by most of the organizations

To be effective, firewalls should allow individual on the corporate network to access the Internet and at the same time, stop hackers or others on the Internet from gaining access to the corporate network to cause damage. Generally, most organizations can follow any of the two philosophies

- Deny-all philosophy -- which means that access to a given recourses will be denied unless a user can provide a specific business reason or need for access to the information resource.
- Accept All Philosophy -- under which everyone is allowed access unless someone can provide a reason for denying access.

Q-Management information system of Howard University contains confidential information about their employees. As all of the information is collected, processed and stored in computers, so, there is the need to set security objectives for Howard University to secure their Management information system. Mention three main security objectives in this regard.

The security objective uses three terms

- Availability – information systems are available and usable when required;
- Confidentiality – data and information are disclosed only to those who have a right to know it; and
- Integrity – data and information are protected against unauthorized modification (integrity).

Q-Identify and list at least three types of Intrusion Detection Systems (IDS).

Another element to securing networks is an intrusion detection system (IDS). IDS is used in complement to firewalls. An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies. It protects a company's information systems resources from external as well as internal misuse.

- Signature-based: These IDS systems protect against detected intrusion patterns. The intrusive patterns they can identify are stored in the form of signatures.
- Statistical-based: These systems need a comprehensive definition of the known and expected behaviour of systems.

• Neural networks: An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database.

2.Analyze the following statements and give the name of active attack described in each case:

• :Duplicating logon procedures and capturing password of a user in such a way that the user thinks that he is interacting with the operating system. Spoofing

• Employing the facilities of the operating system without being subject to the normal controls. Backdoors/trapdoors

• Users run a program which undertakes unauthorized activities e.g. a copy of the sensitive data. Trojan Horse

• Unauthorized user behaves as an authorized user of the system. Piggybacking

• Intercepting, modifying or substituting communications by new message. Masquerading

Q.Passive attacks types any two?

• Network Analysis • Eavesdropping • Traffic Analysis

Q A company's IT security officer noticed unnecessary modifications in database records. What will be the mechanism to identify the person who made unnecessary modifications? Explain this mechanism briefly.

Q what are the reasons that employees don't change in ERP application

I think due to heavy cost

Q how virus is transferred in a computer; name 5 sources through which viruses are transferred

1. Free Software – software downloaded from the net

2. Pirated software – cheaper than original versions

3. Games software – wide appeal and high chances

. Email attachments – quick to spread

5. Portable hard and flash drives – employees take disks home and may work on their own personal PC, which have not been cleaned or have suitable anti-viruses installed on them.

Discuss two Major challenges to Supply Chain and write two sub challenges of each Major challenge.

There are usually two major sources of challenges to supply chains.

1. The uncertainties faced

   a. Demand forecast

   b. Competition

   c. Weather conditions

   d. Technological development

2. The need to coordinate several activities

   a. Business partners are misunderstood

   b. Departments are not well connected

One question of Intrusion Detection Systems.

Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.

What is the difference between Entity and Entity Sets?

An entity is an object that exists and is distinguishable from other objects.

An entity set is a set of entities of the same type that share the same properties.

Q-- identify trojan horse and worm , 2 sentences was given we have to tell which is trojan and which is worm.

A Trojan horse is a malicious program that is disguised as or embedded within legitimate software. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

A Worm is a program which spreads over network connections. This is unlike a virus and does not physically attach itself to another program. Worm typically exploits security weaknesses in operating systems configurations to propagate itself to the host systems.

Q-- write 2 benefit of e-learning.

E-Learning is the online delivery of information for purposes of education, training, knowledge management, or performance management. It is a web - enabled system that makes knowledge accessible to those who need it, when they need it – anytime, anywhere. E-learning is useful for facilitating learning at schools.

Q-- logical threat ?

This refers to damage caused to the software and data without any physical damage to the computers.

Q-- passive attack and three example.

This class of network attacks involves probing for network information. These passive attacks can lead to actual active attacks or intrusions/penetrations into an organization's network. By probing for network information, the intruder obtains network information as that can be used to target a particular system or set of systems during an actual attack.

Types of Passive attacks Examples of passive attacks that gather network information include the following:

- Network Analysis
- Eavesdropping
- Traffic Analysis

Q-- why management shifting their manual work to computerized , give 5 reason.

As advancement was made in every field of life, manual information systems were converted to computerized systems. In manual environment, the concept of transformation was difficult to apply, since input of data into records was by itself the output which also included simple computations. Concept of control mechanism grew stronger as computerized information systems emerged. Now the concept of Information system exists with the usage and benefits of Computers as an inevitable part.

Characteristic of incremental modle?2

- The system development is broken into many mini development projects
- Partial systems are successively built to produce a final total system.
- Highest priority requirements tackled early on.

• Once an incremented portion is developed, requirements for that increment are frozen.

What is the purpose of E-Learning?2

rep

Attacks were given need to identify, is it logic or physical?2

rep

Statement were given, need to identify, it is Technical or non-technical?3

Technical methods are safeguards that are incorporated into computer hardware, software and firmware such as controls mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software, etc.

Non-technical controls are management and operational controls such as security policies and operational procedures and personnel, physical and environmental security.

Types of Intrusion Detection Systems?3

Signature-based: These IDS systems protect against detected intrusion patterns. The intrusive patterns they can identify are stored in the form of signatures.

• Statistical-based: These systems need a comprehensive definition of the known and expected behaviour of systems.

• Neural networks: An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database.

Object oriented programing?3

The concept of object oriented analysis and design focuses on problems in terms of classes and objects.

Two Major challenges and two its sub challenges of supply chain?5

rep

- Identify the following threats as Physical or Logical.

rep

- We will use at least five features that should be available in IDS to make it effective, fully functional and a successful security measure. 5 marks

- There are two types of threat to web security

There is two major classes of security threats

• Passive Attacks

• Active Attacks

- is prototype necessary to build while developing application

Prototyping – Based upon the finalized strategy and the preliminary design, the first prototype of the new system is then developed. This is usually a scaled-down version of the system, and represents an approximation of the characteristics of the final product.

- phases that are required to implement the Change Management (5)

• Shock and Surprise – Confrontation with unexpected situation mostly 1. by accident e.g. loss in a business unit or 2. planned e.g. workshops for personal development

• Denial & Refusal – people express their conviction that change is not necessary

• Rational Understanding – People realize tha need for change and find short term solutions

• Emotional Acceptance – if management succeeds in creating willingness for change, people change their beliefs and behaviour, otherwise change process stops or slows down.

• Exercising & Learning – People start to try new behaviors and processes, as a result will experience success and failures. Change managers should create easier tasks at start to create early wins
• Realization – the knowledge gained in previous phase has feed-back effect.
• Integration – LAST PHASE: total link-up is created between newly acquired patterns of thinking and acting. New behaviors become routine.

- basic processes included in cryptograph

• Encryption – the process of converting data into codes (cryptograms)
• Decryption – the process of decoding the code arrived at data actually encrypted

Q1: Why organization devise great capital for good security policy? one reason?

The organizations interested in raising the security levels of their information system undergo what is commonly termed as "Security Program" or "Security Review". This can be seen as a first attempt to devise a formal security policy for the organization.

Q2: Statement was given identify Worm and Trojan Horse

rep

Q3: Name of manuals required in software design phase?

Q4: ERP is used to integrate information system?

Q5: Name the tools of Structured design and Analysis approach?

Two approaches are followed for system analysis and design

• Structured analysis and design – Which includes various tools, such as.

  • Flowcharting

  • Data Flow diagram

  • ERD

• Object oriented analysis and design

Q6: Object, its form in object oriented programming?

An object can be defined as "A concept, abstraction, or thing with crisp boundaries and meaning of the problem at hand. Objects serve two purposes, they promote understanding of the real world and provide a practical basis for computer implementation."

Q8: Name any six change management phases?

• Shock and Surprise – Confrontation with unexpected situation mostly

  1. by accident e.g. loss in a business unit or

  2. planned e.g. workshops for personal development

• Denial & Refusal – people express their conviction that change is not necessary

• Rational Understanding – People realize tha need for change and find short term solutions

• Emotional Acceptance – if management succeeds in creating willingness for change, people change their beliefs and behaviour, otherwise change process stops or slows down.

• Exercising & Learning – People start to try new behaviours and processes, as a result will experience success and failures. Change managers should create easier tasks at start to create early wins

• Realization – the knowledge gained in previous phase has feed-back effect.

- Integration – LAST PHASE: total link-up is created between newly acquired patterns of thinking and acting. New behaviors become routine. • Integration – LAST PHASE: total link-up is created between newly acquired patterns of thinking and acting. New behaviors become routine.

Q9: Five best password practices, scenario was given?

- Keep the password secret – do not reveal it to anyone
- Do not write it down – if it is complex, people prefer to save it in their cell phone memory, or write on a piece of paper, both of these are not preferred practices.
- Changing password regularly – Passwords should be associated with users not machines. Password generation program can also be used for this purpose.
- Be discreet – it is easy for the onlookers to see which keys are being used, care should be taken while entering the password.
- Do not use obvious password – best approach is to use a combination of letters, numbers, upper case and lower case. Change passes word immediately if you suspect that anyone else knows it.

Q10: Statements was given identify Ethical Issues?

There are certain aspects which when put together formulate a set of ethical issues. These are

1. Privacy issues
2. Accuracy issues
3. Property issues
4. Accessibility issues

Q11: Iterative Model approach, stages and steps involved?

Iterative models are an approach for developing systems based on producing deliverables frequently/repetitively.

- The Initialization step
- The Iteration step
- The Project Control List