FIT2093 Tutorial 12

Topics

- Database Secuirty
- Risk Management

Review Questions Database Security

1. Explain the nature of the **inference** threat to a relational database management system (RDBMS).

   Inference, as it relates to database security, is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received. The inference problem arises when the combination of a number of data items is more sensitive than the individual items, or when a combination of data items can be used to infer data of a higher sensitivity.

2. List and briefly describe two approaches to inference prevention for statistical database.

   Query restriction: Rejects a query that can lead to a compromise. The answers provided are accurate. Perturbation: Provides answers to all queries, but the answers are approximate

3. What are the two main types of statistical databases.

   pure statistical database: just store statistical data
   ordinary database with statistical access: ome users have normal access, others statistical

4. What are the disadvantages to database encryption?

   Key management: Authorized users must have access to the decryption key for the data for which they have access. Because a database is typically accessible to a wide range of users and a number of applications, providing secure keys to selected parts of database to authorized users and applications is complex task. **Inflexibility:** When part or all of the database is encrypted, it becomes more difficult to perform record searching.

5. Imagine that you are the database administrator for a military transportation system. You have a table named cargo in your database that contains information on the various cargo holds available on each outbound airplane . Each row in the table represents a single shipment and lists the contents of that shipment and the flight identification number. Only one shipment per hold is allowed. The flight identification number may be cross-referenced with other tables to determine the origin, destination, flight time, and similar data. the cargo table appears as follows:

Flight ID	Cargo Hold	Contents	Classification
1254	A	Boots	Unclassified
1254	B	Guns	Unclassified
1254	C	Atomic bomb	Top secret
1254	D	Butter	Unclassified

   Suppose that two roles are defined: Role 1 has full access rights to the cargo table. Role 2 has full access rights only to rows of the table in which the Classification field has the

value Unclassified. Describe a scenario in which a user assignment to role 2 uses one or more queries to determine that there is a classified shipment on board the aircraft.

We assume that there is a unique constraint on flight ID and cargo hold (to prevent scheduling two shipments for the same hold).

When a user in role 2 sees that nothing is scheduled for hold C on flight 1254, the user might attempt to insert a new record to transport some vegetables on that flight. However, when he or she attempts to insert the record, the insert will fail due to the unique constraint. At this point, the user has all the data needed to infer that there is a secret shipment on flight 1254. The user could then cross-reference the flight information table to find out the source and destination of the secret shipment and various other information.

Review Questions Risk Management

1. Define IT security management.

   IT security management is a process used to achieve and maintain appropriate levels of

   - confidentiality,
   - integrity,
   - availability,
   - accountability,
   - authenticity and
   - reliability.

   IT security management functions include

   - determining organizational IT security objectives, strategies and policies;
   - determining organizational IT security requirements;
   - identifying and analyzing security threats to IT assets within the organization;
   - identifying and analyzing risks; specifying appropriate safeguards;
   - monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization;
   - developing and implementing a security awareness program; detecting and reacting to incidents.

2. List the steps in the detailed security risk analysis process.

   The steps in the detailed security risk analysis process include:

   - Establish Context or System Characterization,
   - Identify Threats,
   - Identify Vulnerabilities,
   - Analyze Existing Controls,
   - Determine Likelihood,
   - Determine Consequence or Impact on Organization,

- Determine Resulting Risk,
- Document Results in Risk Register,
- Evaluate Risks,
- Treat Risks.

3. Define asset, control, threat, risk and vulnerability. asset: anything that has value to the organization

   - **control:** management, operational and technical processes and procedures that act to reduce the exposure of the organization to some risks
   - **threat:** a potential cause of an unwanted incident that may result in harm to a system or organization risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.
   - **vulnerability:** a weakness in an asset or group of assets that can be exploited by a threat

4. State the two key questions answered to help identify threats and risks for an asset. Briefly indicate how these questions are answered.

   Two key questions which help identify threats and risks for an asset are:

   a. Who or what could cause it harm? and
   b. How could this occur?.

   Answering the first of these questions involves identifying potential threats to assets, which can be natural or man-made, accidental or deliberate. Answering the second of these questions involves identifying flaws or weaknesses in the organizationâĂŹs IT systems or processes, which could be exploited by a threat source to cause harm.

5. Define consequence and likelihood.

   - **consequence:** indicates the impact on the organization should some particular threat actually eventuate, and is typically described qualitatively by the assetâĂŹs owner. This could vary from it being a minor inconvenience (the server was in a branch office, and all data was replicated elsewhere), to a major disaster (the server had the sole copy of all customer and financial records for a small business).
   - **likelihood:** the probability that an identified threat could occur and cause harm to some asset, and is also typically described qualitatively.

6. What is the simple equation for determining risk? Why is this equation not commonly used in practice?

   The simple equation for determining risk is:

   Risk = Probability that threat occurs X Cost to organization

   It is not commonly used in practice because it is often extremely hard to determine accurate probabilities, realistic cost consequences, or both. Hence most risk analysis use qualitative, rather than quantitative, ratings for both these items.

7. With respect to accessing the computer system in your office, list one security requirement that is not realistic, not verifiable.

   a. Non-realistic: zero downtime, no confidentiality loss, perfect security
   b. Non-Verifiable: Reject all or only potential harmful traffic âĂŞ how to know this âĂŞ many only after the security is breached, Maximum protection of privacy.

8. Can you think of two security requirements that are inconsistent or contradictory?

   Full auditing of userâĂŹs action and maintaining the privacy of employees. The first one will lead to the violation of privacy of employees.

9. As part of a formal risk assessment of desktop systems in a small accounting firm with limited IT support, you have identified the asset "integrity of customer financial data files on desktop systems" and the threat "corruption of these files due to import of a worm/virus onto system." Suggest reasonable values for the items in the risk register for this asset and threat, and provide justification for your choices.

   Possible values for the risk register for this asset and threat are:

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
integrity of customer and financial data files on desktop systems	corruption of these files due to import of a worm/virus onto system	anti-virus program	Almost Certain	Major	Extreme

   Given limited IT support, it is likely that the systems and A/V programs are not current, hence given the high rate of worm/virus incidents, infection is almost certain. Similarly, it is likely that such an organization does not regularly backup their data, hence such an infection could cause loss of critical customer/financial data, with serious impact on the organizations functions. Clearly changing these assumptions will change the ratings.

10. As part of a formal risk assessment of the main file server of a small legal firm, you have identified the asset "integrity of the accounting records of the server" and the threat "financial fraud by an employee, disguised by altering the accounting records". Suggest reasonable values for the items in the risk register for this asset and threat, and provide justification for your choices. Possible values for the risk register for this asset and threat are:

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
integrity of the accounting records on the server	Financial fraud by employee, disguised by altering the accounting records	Monthly account audit	Possible	Moderate	High

The chance of insider fraud can be very hard to predict, but is clearly possible. Depending on how long it takes for the fraud to be identified, there could be significant impact on the organizations finances. Assuming there is a regular monthly audit check of the firmâĂŹs cashflow, it is likely the fraud will be detected relatively quickly, which suggests a moderate consequence rating. Again changing these assumptions will change the ratings.