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).
2. List and briefly describe two approaches to inference prevention for statistical database.
3. What are the two main types of statistical databases.
4. What are the disadvantages to database encryption?
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.

Review Questions Risk Management

1. Define IT security management.
2. List the steps in the detailed security risk analysis process.
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.

5. Define consequence and likelihood.

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

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

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

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.

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.