### 

### **3413ICT Network Security**

### **Workshop – 12A**

|  |
| --- |
| **Review Questions:**  The review questions are based on the lecture of database security.   1. By an example, explain why inference attacks rely on certain “metadata”. 2. Consider the following table.     ***RowID***  **Name**  **Position**  **Section**  **Age**  **Gender**  **Salary**  ***R1***  Adam  Officer  Marketing  29  M  48500  ***R2***  Natasha  Manager  Operations  33  F  62000  ***R3***  Sarah  Officer  Operations  27  F  51000  ***R4***  Smith  Clark  Marketing  24  M  42000  ***R5***  Liz  Officer  Operations  27  F  38500  ***R6***  Martha  Officer  Marketing  32  F  44500  ***R7***  Brown  Clark  Marketing  27  M  33000  ***R8***  Carlyle  Manager  Marketing  35  M  58000  ***R9***  Diane  Clark  Operations  30  F  34500  ***R10***  Joe  Officer  Operations  34  M  37500    The salary of a staff is regarded as sensetive information. Any query asking the system to return the salary of an inidividual staff member will be denied. Under this restriction, can you still get the salary of Joe by inference? If so, explain how you can do so.   1. For the same table in Question 2, describe a second method to access Joe’s salary. What extra knowledge would you need for this method to be successful? 2. Name and explain two inference detection approaches. What is the main difference between these two approaches? 3. Differentiate between the two types of statistical databases. Would you think the table given in Question 2 is from a pure statistical database? Why or why not? 4. Explain the following:  * Query restriction * Perturbation      1. Explain why query restriction itself can cause some security issue. 2. Is the query set overlap control a good solution to database security in an e-commerce system for which efficiency is the first priority? Why or why not? 3. Name and explain an attack which can break query size restriction. |

**Challenging task:**

Discuss how eBay database was recently compromised? What were the risks and what controls were in place? Clearly explain how this could have been mitigated? List at least three good references (300 words).