CSC 437/539 Computer Security

Instructor: Dr. Natarajan Meghanathan

Question Bank on Module 8 - Database Security

1) Mention some of the characteristics of "views" of a database table? Why is it not recommended to merge views generated from the same table? Explain with an example. [Hint: Possibility of inference, if we merge views generated from the same table - look at slides 15 and 16 for the example].

2) Consider the breakup of a database master table into three individual tables as shown below. Write SQL statements to create two different views based on the appropriate individual tables (one view listing the Name and Position for those in the **Systems** Department; and another view listing the Salary and Location for those in the **Systems** Department).
(a) Show the tabular results of the individual views.
(b) Combine the results of the two views and show as one single table.
(c) Create the two views as mentioned above; but this time based on the master table and rework parts (a) and (b).

Employee Table

Name	Position	Salary ($)	Department	Location
Andrew	Programmer Analyst	$80,000	Software	Jackson, MS
Robert	Quality Control	$65,000	Software	Memphis, TN
Sheela	Software Developer	$90,000	Software	Atlanta, GA
Victor	Systems Engineer	$75,000	Systems	San Jose, CA
Mary	Systems Administrator	$95,000	Systems	Seattle, WA
Ryan	Network Engineer	$87,000	Systems	Boston, MA

Employee Name - ID Table

Name	Employee ID
Andrew	004
Mary	003
Robert	001
Ryan	005
Sheela	009
Victor	010

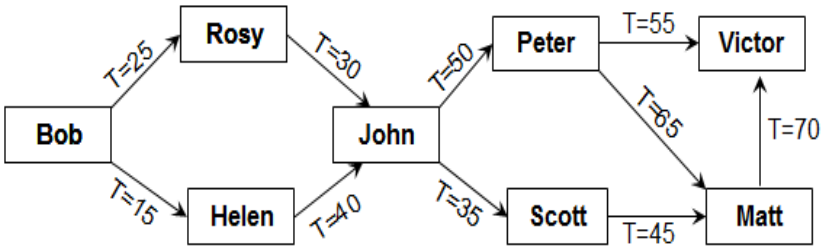
Employee Name Table

Name	Position	Department	Location
Andrew	Programmer Analyst	Software	Jackson, MS
Robert	Quality Control	Software	Memphis, TN
Sheela	Software Developer	Software	Atlanta, GA
Victor	Systems Engineer	Systems	San Jose, CA
Mary	Systems Administrator	Systems	Seattle, WA
Ryan	Network Engineer	Systems	Boston, MA

Salary Table

Employee ID	Salary ($)	Department	Location
001	$65,000	Software	Memphis, TN
003	$95,000	Systems	Seattle, WA
004	$80,000	Software	Jackson, MS
005	$87,000	Systems	Boston, MA
009	$90,000	Software	Atlanta, GA
010	$75,000	Systems	San Jose, CA

3) Consider the chart below that shows the cascading of the "GRANT" authorization. Assume that if a user has received the GRANT permission from more than one user, the user grants the permission to others based on the one received the latest.



(a) Redraw the chart if at time T=60, Bob revokes the permission he gave earlier to Rosy.

(b) Redraw the chart if at time T =75, Bob revokes the permission he gave earlier to Helen.

4) Consider the following database table:

Name	Sex	Major	Class	SAT	GPA
Allen	Female	CS	1980	600	3.4
Baker	Female	EE	1980	520	2.5
Cook	Male	EE	1978	630	3.5
Davis	Female	CS	1978	800	4.0
Evans	Male	Bio	1979	500	2.2
Frank	Male	EE	1981	580	3.0
Good	Male	CS	1978	700	3.8
Hall	Female	IT	1979	580	2.8
Iles	Male	CS	1981	600	3.2
Jones	Female	Bio	1979	750	3.8
Kline	Female	IT	1981	500	2.5
Lane	Male	EE	1978	600	3.0
Moore	Male	CS	1979	650	3.5

Through a sequence of SQL queries, find out GPA of the student named "Good". Explain how would you put together the results of the individual queries to figure out the GPA of the above student.

5) According to the Query Size Restriction technique, for any fixed integer $k > 1$, a query q(C) on a characteristic formula C is allowed if and only if the returned set of records X(C) satisfies $k \leq | X(C) | \leq N - k$. Prove why there needs be an upper bound. You could assume $k = 2$ in your proof.

6) Consider the database table shown above. Using the "Tracker" approach discussed in the module, identify the sets C1 and C2 as well as the tracker T that you would use to infer whether a student named "Good" has a GPA of 3.5 or above. Using D = GPA of 3.5 or above as your filter, write the records for the query sets C1 * D and T * D that you would use as the basis for your inference. Are you impacted by the Query Size restriction constraint to run the above two queries.

Hint:
C1 = Male Size (C1 ^ (GPA >= 3.5) = 3 // **Write the three records**
C2 = CS ^ 1978
~C2 = ~ (CS ^ 1978)
T = C1 ^ ~C2 Size (T ^ GPA >= 3.5) = 2 // **Write the two records**
Show your inference.

7) How does the approach of "Query Set Overlap Control" gets around the vulnerability posed by the Tracker technique? What are the side effects of imposing Query Set Overlap Control?

8) The "Partitioning" technique for Inference control requires that user records have to be inserted or deleted only in pairs.
(a) Explain the need for the above restriction with an example.
(b) Are there any other restrictions for the Partitioning technique? If so, what are they?
(c) Also, what are any side effects of the restrictions of this technique.

9) Assume a database has three attributes X1, X2 and X3 for every record. A user first launches a query to find the sum of these attributes for a record matching a particular constraint and the result returned is 24. The user then launches a query to find the maximum of these three attributes under the same constraint. Why would the Query processor suppress the results of the second query if the maximum of these three attributes turns out to be 8? Justify your answer.

10) With query restriction techniques (that either deny or return an exact answer), the denial of a query may provide sufficient clues that an attacker can deduce underlying information. Give an example to justify this scenario and provide a solution to handle this vulnerability. Indicate any side effects that may exist in your solution.

11) What is the fundamental difference between the query size restriction techniques and the perturbation techniques for inference control?

12) What is the fundamental difference between the two categories of perturbation techniques for inference control?

13) Within the category of "Data Perturbation", we saw two approaches to cause the perturbation on the data. Explain the working of these two approaches with an example for each. Analyze the nature of the errors they introduce.

14) Explain two approaches that we discussed for "Output Perturbation"?

15) Are perturbation techniques preferred for larger databases or smaller databases? Justify your answer.

16) Explain the idea behind the "Binary Encryption" scheme and how it overcomes the problem faced with storing an encrypted version of the records of a table only?. You could use the following table to illustrate the idea.

eid	ename	salary	addr	did
23	Tom	70K	Maple	45
860	Mary	60K	Main	83
320	John	50K	River	50
875	Jerry	55K	Hopewell	92