

Quiz Submissions - Module 6 self-test ▼

Thomas Jun Wei Lim (username: tjwlim)

Attempt 4

Written: Mar 30, 2017 1:16 PM - Mar 30, 2017 1:16 PM

Submission View

Your quiz has been submitted successfully.

Information

Choose the best answer.

Questions

Question 1

1 / 1 point

Which of the following statements is true?

- ☐ In a trigger attack, an attacker derives the answer to a forbidden query by converting the query into multiple allowed queries.
- ☒ PIPEDA is a Canadian law to protect individuals' privacy in their dealings with organizations in the private sector.
- ☐ An integrity lock prevents two conflicting operations from concurrently accessing the same database record.
- ☐ An MLS database stores the results of soccer games.

 [Hide Feedback](#)

Right!

Question 2

1 / 1 point

Which of the following statements are true?

1. In a relational database, there can be multiple records with the same primary key.
2. In a relational database, there can be multiple records with the same foreign key.
3. Any SELECT operation on a view can be expressed as a SELECT operation on the underlying database.
4. Any UPDATE operation on a view can be expressed as an UPDATE operation on the underlying database.

- ☐ 2
- ☐ 2, 3, and 4
- ☒ 2 and 3
- ☐ 1 and 4
- ☐ All of them.

 [Hide Feedback](#)

Right!

Question 3

1 / 1 point

Which of the following statements is true?

- ☐ Logging a user's SELECT queries is sufficient to learn whether the user might have accessed confidential information.
- ☐ The sensitivity of an aggregate is always smaller than the sensitivity of the underlying values.
- ☐ Assume a database has built-in access-control that magically manages to avoid any information leaks in results to user queries. This is sufficient to avoid all information leaks.
- ☒ When anonymizing records in a database with k-anonymity ($k > 1$) before their release, we can do it in such a way that guarantees that an individual cannot be re-identified. (Assume that this release is a one-time operation, so you need not worry about the consequences of multiple such operations.)

Hide Feedback

Right! If the quasi-identifier covers all the record attributes, re-identification will not be possible. Of course, such a large quasi-identifier likely makes the released records useless.

Question 4

1 / 1 point

A database stores three variables x_1 , x_2 , and x_3 , each with a value of 5. The database denies a query if the query allows the requester to deduce the value of a particular variable. Suppose a requester poses the query $\text{sum}(x_1, x_2, x_3)$ and the response is 15. Next, the requester poses the query $\text{max}(x_1, x_2, x_3)$. Which action should the database take?

- ☐ Answer the query.
- ☐ Deny the query.
- ☒ Neither of them.

Hide Feedback

Right! Both answering and denying the query leaks the values of all variables. Of course, avoiding this leak in practice is hard.

Question 5

1 / 1 point

A database stores employees' names and their salaries. The salary information is encrypted with a symmetric cipher in ECB mode and a single encryption key. Which of the following queries do not require decryption of all the records in the database?

1. `SELECT name WHERE salary = 50,000;`
2. `SELECT COUNT(name) WHERE salary = 50,000;`
3. `SELECT COUNT(name) WHERE salary > 50,000;`
4. `SELECT AVG(salary);`

- ☐ 3 and 4
- ☐ 2 and 3
- ☒ 1 and 2
- ☐ 1 and 4

👉 [Hide Feedback](#)

Right! With the given encryption scheme, we can encrypt 50,000 and directly execute the queries.

Question 6

1 / 1 point

Which of the following operations on database records do not help to achieve k-anonymity?

- ☐ Replace postal code with province.
- ☒ Replace last name with its SHA-256 hash
- ☐ Omit street address.

👉 [Hide Feedback](#)

Right! There are no known SHA-256 collisions, so an attacker can simply compute the SHA-256 hash of the last names stored in any additional databases that he/she uses for re-identification and proceed as if the last name had not been hashed.

Attempt Score: 6 /

Overall Grade (last attempt): 6 /

Done