21

SECURITY

Exercise 21.1 Briefly answer the following questions:

1. Explain the intuition behind the two rules in the Bell-LaPadula model for mandatory access control.
2. Give an example of how covert channels can be used to defeat the Bell-LaPadula model.
3. Give an example of polyinstantiation.
4. Describe a scenario in which mandatory access controls prevent a breach of security that cannot be prevented through discretionary controls.
5. Describe a scenario in which discretionary access controls are required to enforce a security policy that cannot be enforced using only mandatory controls.
6. If a DBMS already supports discretionary and mandatory access controls, is there a need for encryption?
7. Explain the need for each of the following limits in a statistical database system:
   (a) A maximum on the number of queries a user can pose.
   (b) A minimum on the number of tuples involved in answering a query.
   (c) A maximum on the intersection of two queries (i.e., on the number of tuples that both queries examine).
8. Explain the use of an audit trail, with special reference to a statistical database system.
9. What is the role of the DBA with respect to security?
10. Describe AES and its relationship to DES.

11. What is public-key encryption? How does it differ from the encryption approach taken in the Data Encryption Standard (DES), and in what ways is it better than DES?

12. Explain how a company offering services on the Internet could use encryption-based techniques to make its order-entry process secure. Discuss the role of DES, AES, SSL, SET, and digital signatures. Search the Web to find out more about related techniques such as *electronic cash*.

Answer 21.1 The answer to each question is given below.

1. The *Simple Security Property* states that subjects can only interact with objects with a lesser or equal security class. This ensures subjects with low security classes from accessing high security objects. The **-Property* states that subjects can only create objects with a greater or equal security class. This prevents a high security subject from mistakenly creating an object with a low security class (which low security subjects could then access!).

2. One example of a covert channel is in statistical databases. If a malicious subject wants to find the salary of a new employee, and can issue queries to find the average salary in a department, and the total number of current employees in the depatment, then the malicious subject can calculate the new employees salary based on the increase in average salary and number of employees.

3. Say relation R contains the following values:

cid	*carname*	Security Class
1	Honda	U
1	Porsche	C
2	Toyota	C
3	Mazda	C
3	Ferrari	TS

   Then subjects with security class U will see R as:

cid	*carname*	Security Class
1	Honda	U

   Subjects with security class C will see R as:

cid	*carname*	Security Class
1	Honda	U
1	Porsche	C
2	Toyota	C
3	Mazda	C

Subjects with security class TS will see R as:

cid	*carname*	Security Class
1	Honda	U
1	Porsche	C
2	Toyota	C
3	Mazda	C
3	Ferrari	TS

4. Trojan horse tables are an example where discretionary access controls are not sufficient. If a malicious user creates a table and has access to the source code of some other user with privileges to other tables, then the malicious user can modify the source code to copy tuples from privileged tables to his or her non-privileged table.

5. Manditory access controls do not distinguish between people in the same clearance level so it is not possible to limit permissions to certain users within the same clearance level. Also, it is not possible to give only insert or select privileges to different users in the same level: all users in the same clearance level have select, insert, delete and update privileges.

6. Yes, especially if the data is transmitted over a network in a distributed environment. In these cases it is important to encrypt the data so people 'listening' on the wire cannot directly access the information.

7. (a) If a user can issue an unlimited number of queries, he or she can repeatedly decompose statistical information by gathering the statistics at each level (for example, at age ¿ 20, age ¿ 21, etc.).

   (b) If a malicious subject can query a database and retrieve single rows of statistical information, he or she may be able to isolate sensitive information such as maximum and minimum values.

   (c) Often the information from two queries can be combined to deduce or infer specific values. This is often the case with average and total aggregates. This can be prevented by restricting the tuple overlap between queries.

8. The *audit trail* is a log of updates with the authorization id of the user who issued the update. Since it is possible to infer information from statistical databases using repeated queries, or queries that target a common set of tuples, the DBA can use an audit trail to see which people issued these security-breaking queries.

9. The DBA creates new accounts, ensures that passwords are safe and changed often, assigns mandatory access control levels, and can analyze the audit trail to look for security breaches. They can also assist users with their discretionary permissions.

10. Public-key encryption is an encryption scheme that uses a public encryption key and a private decryption key. These keys are part of one-way functions whose inverse is very difficult to determine (which is why large prime numbers are involved in encryption algorithms...factoring is difficult!). The public key and private key are inverses which allow a user to encrypt any information, but only the person with the private key can decode the messages. DES has only one key and a specific decrypting algorithm. DES decoding can be more difficult and relies on only one key so both the sender and the receiver must know it.

11. A one-way function is a mathematical function whose inversese is very difficult to determine. These are used to determine the public and private keys, and to do the actual decoding: a message is encoding using the function and is decoded using the inverse of the function. Since the inverse is difficult to find, the code can not be broken easily.

12. An internet server could issue each user a public key with which to encrypt his or her data and send it back to the server (which holds all of the private keys). This way users cannot decode other users' messages, and even knowledge of the public key is not sufficient to decode the message. With DES, the encryption key is used both in encryption and decryption so sending keys to users is risky (anyone who intercepts the key can potentially decode the message).

Exercise 21.2 You are the DBA for the VeryFine Toy Company and create a relation called Employees with fields *ename*, *dept*, and *salary*. For authorization reasons, you also define views EmployeeNames (with *ename* as the only attribute) and DeptInfo with fields *dept* and *avgsalary*. The latter lists the average salary for each department.

1. Show the view definition statements for EmployeeNames and DeptInfo.

2. What privileges should be granted to a user who needs to know only average department salaries for the Toy and CS departments?

3. You want to authorize your secretary to fire people (you will probably tell him whom to fire, but you want to be able to delegate this task), to check on who is an employee, and to check on average department salaries. What privileges should you grant?

4. Continuing with the preceding scenario, you do not want your secretary to be able to look at the salaries of individuals. Does your answer to the previous question ensure this? Be specific: Can your secretary possibly find out salaries of *some* individuals (depending on the actual set of tuples), or can your secretary always find out the salary of any individual he wants to?

5. You want to give your secretary the authority to allow other people to read the EmployeeNames view. Show the appropriate command.

6. Your secretary defines two new views using the EmployeeNames view. The first is called AtoRNames and simply selects names that begin with a letter in the range A to R. The second is called HowManyNames and counts the number of names. You are so pleased with this achievement that you decide to give your secretary the right to insert tuples into the EmployeeNames view. Show the appropriate command and describe what privileges your secretary has after this command is executed.

7. Your secretary allows Todd to read the EmployeeNames relation and later quits. You then revoke the secretary's privileges. What happens to Todd's privileges?

8. Give an example of a view update on the preceding schema that cannot be implemented through updates to Employees.

9. You decide to go on an extended vacation, and to make sure that emergencies can be handled, you want to authorize your boss Joe to read and modify the Employees relation and the EmployeeNames relation (and Joe must be able to delegate authority, of course, since he is too far up the management hierarchy to actually do any work). Show the appropriate SQL statements. Can Joe read the DeptInfo view?

10. After returning from your (wonderful) vacation, you see a note from Joe, indicating that he authorized his secretary Mike to read the Employees relation. You want to revoke Mike's `SELECT` privilege on Employees, but you do not want to revoke the rights you gave to Joe, even temporarily. Can you do this in SQL?

11. Later you realize that Joe has been quite busy. He has defined a view called AllNames using the view EmployeeNames, defined another relation called StaffNames that he has access to (but you cannot access), and given his secretary Mike the right to read from the AllNames view. Mike has passed this right on to his friend Susan. You decide that, even at the cost of annoying Joe by revoking some of his privileges, you simply have to take away Mike and Susan's rights to see your data. What `REVOKE` statement would you execute? What rights does Joe have on Employees after this statement is executed? What views are dropped as a consequence?

Answer 21.2

1. EmployeeNames and DeptInfo are defined below:

```
CREATE VIEW EmployeeNames (ename)
       AS SELECT E.ename
          FROM   Employees E
```

```
CREATE VIEW DeptInfo (dept, avgsalary)
       AS SELECT   DISTINCT E.dept, AVG (E.salary) AS avgsalary
          FROM     Employees E
          GROUP BY E.dept
```

2. `SELECT` privilege on the `VIEW` DeptInfo.

   Note that it is impossible to allow the user to access only the average salaries of 'Toy' and 'CS' departments but not those of the other departments. If we really want the average salaries of other departments to be hidden from this user, we have no choice but to create another view.

3. a) `DELETE` on Employees
   b) `SELECT` on EmployeeNames
   c) `SELECT` on DeptInfo

4. No it does not ensure that. It is not possible for the secretary to find out the salary of any employee using just the relations alone.
   If the tuples are such that there is just one employee in a department and the secretary knows this information along with the name of the employee who works there, then he can possibly find out the salary. However, the relations themselves do not allow the secretary to deduce such a fact.

5. `GRANT SELECT ON` Employees `TO` Secretary `WITH GRANT OPTION`

6. `GRANT INSERT ON` Employees `TO` Secretary
   The secretary can now also insert tuples into AtoRNames, which is an updatable view created by the secretary. However, the secretary still cannot insert tuples into HowManyNames because this view is not updatable.

7. Todd's privileges are also revoked.

8. One example of a view update that cannot be implemented through updates to Employees is changing the average salary for a department since one doesn't know which salaries to change.

9. `GRANT SELECT, INSERT, UPDATE ON` Employees `TO` Joe `WITH GRANT OPTION`
   `GRANT SELECT, INSERT, UPDATE ON` EmployeeNames `TO` Joe `WITH GRANT OPTION`
   Joe cannot read the DeptInfo view, but could an identical view.

10. There is no way to do this in SQL: even though you granted privileges to Joe and Joe granted privileges to Mike, you cannot revoke Joe's privileges without also revoking Mike's.

11. Since you don't own AllNames, you can only prevent Mike and Susan from accessing it by revoking Joe's right to read EmployeeNames:

`REVOKE SELECT ON` EmployeeNames `FROM` Joe
The view AllNames is dropped as a consequence. Joe can still modify EmployeeNames without reading it.

Exercise 21.3 You are a painter and have an Internet store where you sell your paintings directly to the public. You would like customers to pay for their purchases with credit cards, and wish to ensure that these electronic transactions are secure.

Assume that Mary wants to purchase your recent painting of the Cornell Uris Library. Answer the following questions.

1. How can you ensure that the user who is purchasing the painting is really Mary?
2. Explain how SSL ensures that the communication of the credit card number is secure. What is the role of a certification authority in this case?
3. Assume that you would like Mary to be able to verify that all your email messages are really sent from you. How can you authenticate your messages without encrypting the actual text?
4. Assume that your customers can also negotiate the price of certain paintings and assume that Mary wants to negotiate the price of your painting of the Madison Terrace. You would like the text of this communication to be private between you and Mary. Explain the advantages and disadvantages of different methods of encrypting your communication with Mary.

Answer 21.3 The answer to each question is given below.

1. In order to determine whether the user who is purchasing the painting is really Mary, we need some level of verification when Mary first registers with the system. On the lowest level, we can simply ask the user to confirm things like Mary's address or social security number. To increase the level of security, we could also ask the user to verify Mary's credit card number. Since these numbers are deemed difficult to obtain, most merchant websites consider this sufficient evidence for proof of identity.

   For an even higher level of security, we can take external steps to verify Mary's information such as calling her up with the phone number provided, sending a letter to Mary's mailing address, or sending her an e-mail with instructions to reply back. In each instance, we attempt to validate the information the user provided so that the element of uncertainty in the provided information is decreased.

2. SSL Encryption is a form of public-key encryption where a third party certification authority acts to validate public keys between two clients. In a general public-key