**ĐỀ CƯƠNG ÔN TẬP**

HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

-------------------

**“AN TOÀN CƠ SỞ DỮ LIỆU”**

*Giảng viên: Trần Thị Lượng*

**Chương 1: Tổng quan về an toàn thông tin trong CSDL**

1. Các mối đe dọa, các tấn công có thể đến với CSDL là gì?

2. Tìm hiểu các cấu hình xử lý CSDL (CSDL tập trung, phân tán, Client/Server). Các cấu hình này được áp dụng như thế nào trong thực tế. (Chú ý: nêu rõ đặc điểm – bản chất và vẽ hình minh họa).

3. Trình bày về SQL, các câu lệnh SQL cơ bản.

4. Trình bày các yêu cầu bảo vệ CSDL .

5. Trình bày một số phương pháp (được tích hợp sẵn trong các DBMS) để đảm bảo tính toàn vẹn dữ liệu.

6. Tìm hiểu về Transaction và quá trình thực hiện một Transaction.

**Chương 2. Các mô hình và chính sách an toàn**

1. Nêu rõ đặc điểm của kiểm soát truy nhập MAC và DAC trong CSDL, nêu sự khác nhau giữa chúng. Ứng dụng 2 chính sách này trong thực tế các hệ quản trị như thế nào?

Trình bày về hệ thống Multilevel security: đ/n, các đặc điểm chính, ví dụ.

2. Thế nào là mô hình an toàn? Sự khác nhau giữa mô hình an toàn và chính sách an toàn. Tìm hiểu mô hình an toàn là Bell-Lapadula.

3. Trình bày cơ bản về một số phương pháp có thể bảo vệ CSDL trong hệ quản trị Oracle (chẳng hạn: VPD, mã hóa CSDL, OLS, Kiểm toán…), các phương pháp đảm bảo tính toàn vẹn CSDL trong DBMS.

4. Trình bày những lớp người dùng chính của một hệ thống an toàn CSDL và vai trò của họ.

5. Trình bày việc gán/thu hồi quyền trong MAC và DAC.

6. Trình bày đặc điểm cơ bản về mô hình RBAC.

7. Tìm hiểu mô hình cấp quyền System R, bộ quyền trong System R. Đặc biệt lưu ý vấn đề thu hồi quyền đệ quy và không đệ quy.

1. Nêu ví dụ về đặc quyền hệ thống (System Prilvilege) và đặc quyền đối tượng (Object Prilvilege), viết câu lệnh SQL cho các ví dụ đó. Nêu sự khác nhau giữa Admin option và Grant option. (Ví dụ các câu lệnh SQL).
2. Đặc điểm cơ bản của hai phương pháp kiểm soát phụ thuộc dữ liệu gồm: Kiểm soát truy cập dựa trên khung nhìn và Sửa đổi truy vấn.
3. **Khái niệm về chủ thể an toàn và đối tượng an toàn trong mô hình an toàn CSDL. Kể tên các mô hình an toàn CSDL và lấy ví dụ.**

**Chương 3. An toàn trong DBMS**

- Tìm hiểu đặc điểm cơ bản của kiến trúc chủ thể tin cậy (Trusted Subject) và kiến trúc Integrity Lock. Đặc biệt chú ý kiến trúc Intergrity Lock (cả lý thuyết và bài tập).

- Tìm hiểu kỹ về khái niệm và ý tưởng của tấn công SQL Injection

- Các đặc điểm khác nhau giữa DBMS và OS

- Những đặc điểm cơ bản của Kiến trúc Trusted Subject và Kiến trúc Woods Hole.

- Các đặc điểm cơ bản của ba cơ chế: Xác thực, ủy quyền và kiểm toán trong các DBMS.

**Chương 4. Ứng dụng mật mã trong AT CSDL**

- Nêu các lợi ích, nguyên tắc và tác động của việc mã hóa dữ liệu đối với một tổ chức, doanh nghiệp

- Các chiến lược mã hóa CSDL (mã hóa bên trong DBMS và bên ngoài DBMS)

- Tìm hiểu những vấn đề cần thiết khi mã hóa CSDL (vấn đề mã hóa ở đâu, bảo vệ khóa, phân phối khóa như thế nào…)

**Chương 5 Cơ sở dữ liệu thống kê**

1. Cơ sở dữ liệu thống kê (statistical database) là gì? (Viết được các câu lệnh SQL cho các thống kê). Ứng dụng trong thực tế? Các dạng biểu diễn.
2. Tìm hiểu những khái niệm cơ bản trong CSDL thống kê.
3. Thế nào là thống kê nhạy cảm, cho ví dụ? Working knowledge và Supplementary knowledge?
4. Nêu đặc điểm cơ bản về Tấn công dựa vào Trình theo dõi (trình bày được ý tưởng của 2 kiểu tấn công này) và cho ví dụ.
5. Kể tên các tấn công suy diễn vào SDB và lấy ví dụ về tấn công dựa vào đếm.
6. Giải thích tấn công suy diễn “Interference attack”, lấy ví dụ về tấn công này.
7. Có những dạng biểu diễn nào của một SDB, giải thích từng dạng biểu diễn này và cho ví dụ đơn giản.
8. Trình theo dõi (Tracker)? Trình bày sự khác nhau giữa hai kiểu tấn công trình theo dõi (kiểu 1 và kiểu 2).
9. Ưu, nhược điểm của Kiểm soát kích cỡ tập truy vấn với SDB.
10. Đặc điểm cơ bản của Kỹ thuật giấu ô.
11. Ưu, nhược điểm của kỹ thuật giấu ô và kỹ thuật gây nhiễu dữ liệu.
12. Công thức đặc trưng là gì*.* Hãy viết các câu truy vấn ví dụ về Count, Sum, Min trên C.
13. So sánh, vẽ hình hai kỹ thuật gây nhiễu dữ liệu.
14. Tìm hiểu các kỹ thuật chống suy diễn trong CSDL thống kê, nêu ưu nhược điểm của từng phương pháp. (Chú ý tìm hiểu kỹ các kiểm soát này)
    * Kiểm soát kích cỡ tập truy vấn
    * Kỹ thuật giấu ô
    * Kỹ thuật gây nhiễu

**Chương 6. Kiểm toán + Phát hiện xâm nhập CSDL**

- Vai trò và các cơ chế kiểm toán cơ bản cho CSDL

- Trình bày đặc điểm của mô hình phát hiện xâm nhập CSDL dựa trên bất thường và mô hình phát hiện xâm nhập CSDL dựa trên lạm dụng. Vẽ mô hình Kiến trúc của một IDS CSDL bao gồm cả hai mô hình phát hiện trên.

- Vẽ hình mô tả và giải thích hai giai đoạn: giai đoạn đào tạo và giai đoạn phát hiện của một hệ thống phát hiện xâm nhập cơ sở dữ liệu dựa trên bất thường.

**BÀI TẬP:**

Lưu ý một số dạng bài tập sau:

* Bài tập chương 5 về tấn công suy diễn và kỹ thuật giấu ô
* Bài tập chương 3 về Gắn tem, giải thích tại sao đảm bảo được tính toàn vẹn cho CSDL bằng kỹ thuật Intergrity Lock
* Bài tập về Multilevel Security + Bellapadula.
* Đề thi có thể có một vài ý nhỏ mở rộng ko nằm trong đề cương.

**LƯU Ý:**

* + **Sinh viên cần nắm rõ các câu lệnh SQL để minh họa cho các phần đã đề cập (đặc biệt trong các tấn công thống kê chương 5 phải viết được các câu lệnh SQL thực hiện cho cả quá trình tấn công), ngoài ra mỗi phần có thể cần hình vẽ để minh họa.**
  + **Đề thi không được sử dụng tài liệu**
  + **Nếu sinh viên chép bài của nhau đều bị 0 điểm.**