Bài 13: Bảo mật thông tin trong các hệ cơ sở dữ liệu

A. Lý thuyết

Bảo mật là vấn đề chung cho cả hệ CSDL và những hệ thống khác, bảo mật trong CSDL là:

• Ngăn chặn các truy cập không được phép;

• Hạn chế tối đa các sai sót của người dùng;

• Đảm bảo thông tin không bị mất hoặc bị thay đổi ngoài ý muốn;

• Không tiết lộ nội dung dữ liệu cũng như chương trình xử lí;

• Các giải pháp chủ yếu cho bảo mật hệ thống là chính sách và ý thức, phân quyền truy cậpvà nhận dạng người dùng, mã hoá thông tin và nén dữ liệu, lưu biên bản.

1. Chính sách và ý thức

Việc bảo mật có thể thực hiện bằng các giải pháp kĩ thuật cả phần cứng lẫn phần mềm. Tuy nhiên hiệu quả việc bảo mật phụ thuộc rất nhiều vào các chủ trương, chính sách của chủ sở hữu thông tin và ý thức của người dùng.

• Ở cấp quốc gia: bảo mật phụ thuộc vào sự quan tâm của chính phủ trong việc ban hành các chủ trương, chính sách, điều luật qui định của nhà nước. Cần có các quy định cụ thể cho việc bảo vệ an toàn thông tin.

• Người phân tích, thiết kế và người QTCSDL: phải có các giải pháp tốt về phần cứng và phần mềm thích hợp.

• Người dùng cần có ý thức coi thông tin là một tài nguyên quan trọng, cần có trách nhiệm cao.

2. Phân quyền truy cập và nhận dạng người dùng

• Tuỳ theo vai trò khác nhau mà người dùng được phân quyền khác nhau để truy cập CSDL.

• Bảng phân quyền truy cập cũng là dữ liệu của CSDL, được tổ chức và xây dựng như những dữ liệu khác. Được quản lí chặt chẽ, không giới thiệu công khai, chỉ có người quản trị hệ thống được cập nhật.

• Bảng phần quyền truy cập có dạng sau:

	Mã HS	Các điểm số	Các thông tin khác
K10	Đ	Đ	K
K11	Đ	Đ	K
K12	Đ	Đ	K
Giáo viên	Đ	Đ	Đ
Người quản trị	ĐSBX	ĐSBX	ĐSBX

• Hệ QTCSDL phải nhận biết được người dùng, giải pháp là dùng mật khẩu hoặc chữ kí điện tử.

• Người QTCSDL cần cung cấp:

+ Bảng phân quyền truy cập cho hệ CSDL.

+ Phương tiện cho người dùng hệ QTCSDL nhận biết đúng được họ.

+ Người dùng muốn truy cập vào hệ thống cần khai báo:

+ Tên người dùng.

+ Mật khẩu.

• Dựa vào hai thông tin này, hệ QTCSDL xác minh để cho phép hoặc từ chối quyền truy cập CSDL.

• Dựa vào hai thông tin này, hệ QTCSDL xác minh để cho phép hoặc từ chối quyền truy cập CSDL (chẳng hạn khai báo đúng tên người dùng nhưng không đúng mật khẩu của người dùng đó).

• Lưu ý:

+ Đối với nhóm người truy cập cao thì cơ chế nhận dạng có thể phức tạp hơn.

+ Hệ QTCSDL cung cấp cho người dùng cách thay đổi mật khẩu, tăng cường khả năng bảo vệ mật khẩu.

3. (Giảm tải – Học sinh tự học) **Mã hóa thông tin và nén dữ liệu**

• Các thông tin quan trọng và nhạy cảm thư¬ờng được lưu trữ dưới dạng mã hoá để giảm khả năng rò rỉ. Có nhiều cách mã hoá khác nhau, tiêu biểu là nén dữ liệu để giảm dung lượng bộ nhớ lưu trữ dữ liệu.

• Mã hóa độ dài loạt là một cách nén dữ liệu khi trong tệp dữ liệu có các kí tự được lặp lại liên tiếp.

• Ngoài mục đích giảm dung lượng lưu trữ, nén dữ liệu cũng góp phần tăng cường tính bảo mật của dữ liệu. Khi có dữ liệu dạng nén, cần biết quy tắc nén mới có dữ liệu gốc được.

• Lưu ý: Các bản sao dữ liệu thường được mã hóa và nén bằng các chương trình riêng.

4. (Giảm tải – Học sinh tự học) **Lưu biên bản**

• Ngoài các giải pháp nêu trên người ta còn tổ chức lưu biên bản hệ thống, thông thường biên bản hệ thống cho biết:

+ Số lần truy cập vào hệ thống, vào từng thành phần của hệ thống, vào từng yêu cầu tra cứu,...

+ Thông tin về số lần cập nhật cuối cùng: phép cập nhật, người thực hiện, thời điểm cập nhật,...

• Biên bản hệ thống hỗ trợ cho việc khôi phục hệ thống khi có sự cố kĩ thuật, cung cấp thông tin cho phép đánh giá mức độ quan tâm của người dùng đối với hệ thống

• Dựa vào biên bản người quản trị có thể phát hiện những truy cập bất thường.

• Có nhiều yếu tố của hệ thống bảo vệ có thể thay đổi trong quá trình khai thác hệ CSDL

• Để nâng cao hiệu quả bảo mật, các tham số của hệ thống bảo vệ phải thư¬ờng xuyên được thay đổi.

• Lưu ý: hiện nay các giải pháp cả phần cứng lẫn phần mềm chưa đảm bảo hệ thống được bảo vệ an toàn tuyệt đối.

B. Trắc nghiệm

Câu 1: Phát biểu nào dưới đây không phải là bảo mật thông tin trong hệ CSDL?

A. Ngăn chặn các truy cập không được phép

B. Hạn chế tối đa các sai sót của người dùng

C. Đảm bảo thông tin không bị mất hoặc bị thay đổi ngoài ý muốn

D. Khống chế số người sử dụng CSDL

Câu 2: Các giải pháp cho việc bảo mật CSDL gồm có:

A. Phân quyền truy cập, nhận dạng người dùng, mã hoá thông tin và nén dữ liệu, lưu biên bản.

B. Phân quyền truy cập, nhận dạng người dùng, mã hoá thông tin và nén dữ liệu, chính sách và ý thức, lưu biên bản, cài đặt mật khẩu

C. Nhận dạng người dùng, mã hoá thông tin và nén dữ liệu, chính sách và ý thức, lưu biên bản.

D. Phân quyền truy cập, nhận dạng người dùng; mã hoá thông tin và nén dữ liệu; chính sách và ý thức; lưu biên bản.

Câu 3: Bảng phân quyền cho phép :

A. Phân các quyền truy cập đối với người dùng

B. Giúp người dùng xem được thông tin CSDL.

C. Giúp người quản lí xem được các đối tượng truy cập hệ thống.

D. Đếm được số lượng người truy cập hệ thống.

Câu 4: Người có chức năng phân quyền truy cập là:

A. Người dùng

B. Người viết chương trình ứng dụng.

C. Người quản trị CSDL.

D. Lãnh đạo cơ quan.

Câu 5: Trong các phát biểu sau, phát biểu nào sai ?

A. Bảng phân quyền truy cập cũng là dữ liệu của CSDL

B. Dựa trên bảng phân quyền để trao quyền truy cập khác nhau để khai thác dữ liệu cho các đối tượng người dùng khác nhau

C. Mọi người đều có thể truy cập, bổ sung và thay đổi bảng phân quyền

D. Bảng phân quyền không giới thiệu công khai cho mọi người biết

Câu 6: Trong một trường THPT có xây dựng một CSDL quản lý điểm Học Sinh. Người Quản trị CSDL có phân quyền truy cập cho các đối tượng truy cập vào CSDL. Theo em cách phân quyền nào dưới đây hợp lý:

A. HS: Xem; GVBM: Xem, Bổ sung; BGH: Xem, sửa, xoá.

B. HS: Xem; GVBM: Xem, Bổ sung, sửa, xóa; BGH: Xem, Bổ sung.

C. HS: Xem; GVBM: Xem, Bổ sung, sửa, xoá; BGH: Xem.

D. HS: Xem, Xoá; GVBM: Xem, Bổ sung, sửa, xoá; BGH: Xem, Bổ sung, sửa, xoá.

Câu 7: Các yếu tố tham gia trong việc bảo mật hệ thống như mật khẩu, mã hoá thông tin cần phải:

A. Không được thay đổi để đảm bảo tính nhất quán.

B. Chỉ nên thay đổi nếu người dùng có yêu cầu.

C. Phải thường xuyên thay đổi để tăng cường tính bảo mật.

D. Chỉ nên thay đổi một lần sau khi người dùng đăng nhập vào hệ thống lần đầu tiên.

Câu 8: Thông thường, người dùng muốn truy cập vào hệ CSDL cần cung cấp:

A. Hình ảnh.

B. Chữ ký.

C. Họ tên người dùng.

D. Tên tài khoản và mật khẩu.

Câu 9: Câu nào sai trong các câu dưới đây khi nói về chức năng lưu biên bản hệ thống?

A. Cho biết số lần truy cập vào hệ thống, vào từng thành phần của hệ thống, vào từng yêu cầu tra cứu, ...

B. Cho thông tin về một số lần cập nhật cuối cùng

C. Lưu lại nội dung cập nhật, người thực hiện, thời điểm cập nhật

D. Lưu lại các thông tin cá nhân của người cập nhật

Câu 10: Để nâng cao hiệu quả của việc bảo mật, ta cần phải:

A.Thường xuyên sao chép dữ liệu

B.Thường xuyên thay đổi các tham số của hệ thống bảo vệ

C.Thường xuyên nâng cấp phần cứng, phần mềm

D. Nhận dạng người dùng bằng mã hoá