Nội dung

- Điều khiển dữ liệu phân tán
  - Quản lý khung nhìn
  - Bảo mật dữ liệu
  - Kiểm soát toàn vẹn ngữ nghĩa

Bảo mật dữ liệu

- Bảo vệ dữ liệu
  - Ngăn chặn người dùng trái phép hiểu được nội dung vật lý của dữ liệu
  - Sử dụng các kỹ thuật mã hóa/giải mã (Khóa công khai)
- Điều khiển truy nhập
  - Chỉ những người dùng được phép/ủy quyền mới được thực hiện các thao tác (mà họ được cho phép thực hiện) trên các đối tượng CSDL.
  - Kiểm soát truy nhập tùy ý (Discretionary access control - DAC)
    - Từ lâu đã được cung cấp bởi các hệ quản trị CSDL với các quy tắc ủy quyền.
  - Kiểm soát truy nhập đa mức (Multilevel access control - MAC)
    - Tăng cường bảo mật với nhiều mức

Kiểm soát truy nhập tùy ý

- Các tác nhân chính
  - Chủ thể (người dùng, nhóm người dùng) thực hiện thao tác
  - Các thao tác (trong các câu truy vấn hoặc chương trình ứng dụng)
  - Các đối tượng, trên đó các thao tác được thực hiện
- Kiểm tra xem một chủ thể có thể thực hiện một thao tác trên một đối tượng hay không
  - Ủy quyền = (chủ thể, loại thao tác, đối tượng)
  - Được xác định bằng: GRANT hoặc REVOKE
  - Tập trung: một lớp người dùng đơn (quản trị) có thể được cấp hoặc thu hồi quyền
  - Không tập trung, với loại tùy chọn GRANT
    - Tiến trình thu hồi đệ quy linh hoạt hơn nhưng cần có hệ thống phân quyền

Vấn đề với kiểm soát truy nhập tùy ý

- Người dùng xấu có thể truy nhập dữ liệu trái phép thông qua người dùng được ủy quyền.
- Ví dụ
  - Người dùng A có quyền truy nhập vào *R* và *S*
  - Người dùng B chỉ có quyền truy nhập vào *S*
  - B bằng cách nào đó có thể sửa đổi một chương trình ứng dụng được A sử dụng để ghi dữ liệu *R* vào *S*
  - Khi đó B có thể đọc dữ liệu trái phép (trong *S*) mà không vi phạm quy tắc ủy quyền.
- Giải pháp: sử dụng bảo mật đa mức (ví dụ, dựa trên mô hình Bell và Lapuda nổi tiếng về bảo mật hệ điều hành).

Kiểm soát truy nhập đa mức

- Các mức bảo mật khác nhau
  - *Top Secret > Secret > Confidential > Unclassified*
    (Tuyệt mật) (Bí mật) (Bảo mật) (Chưa được phân loại)
- Điều khiển truy nhập bởi 2 quy tắc:
  - Không đọc lên
    - Chủ thể *S* chỉ được phép đọc đối tượng mức *L* nếu *level(S) ≥ L*
    - Bảo vệ dữ liệu khỏi bị tiết lộ trái phép, ví dụ: một chủ thể được cấp quyền bí mật không thể đọc được dữ liệu tuyệt mật.
  - Không ghi lại
    - Chủ thể *S* chỉ được phép ghi một đối tượng mức *L* nếu *level(S) ≤ L*
    - Bảo vệ dữ liệu khỏi sự thay đổi trái phép, ví dụ: một chủ thể được cấp quyền tuyệt mật chỉ có thể ghi dữ liệu tuyệt mật chứ không phải dữ liệu bí mật (khi đó có thể chứa dữ liệu tuyệt mật).

Kiểm soát truy nhập đa mức trong CSDL quan hệ

- Một quan hệ có thể được phân loại theo các mức bảo mật khác nhau
  - Quan hệ: tất cả các bộ dữ liệu có cùng mức bảo mật
  - Bộ: Mỗi bộ có một mức bảo mật
  - Thuộc tính: Mỗi thuộc tính có một mức bảo mật
- Do đó, một quan hệ được phân thành nhiều mức
  - Xuất hiện khác nhau (với dữ liệu khác nhau) đối với các chủ thể có các mức bảo mật khác nhau.

Ví dụ

PROJ*: Được phân loại bảo mật theo thuộc tính

PNO	SL1	PNAME	SL2	BUDGET	SL3	LOC	SL4
P1	C	Instrumentation	C	150000	C	Montreal	C
P2	C	DB Develop.	C	135000	S	New York	S
P3	S	CAD/CAM	S	250000	S	New York	S

PROJ* được nhìn thấy bởi một chủ thể có quyền bảo mật (mức *C*)

PNO	SL1	PNAME	SL2	BUDGET	SL3	LOC	SL4
P1	C	Instrumentation	C	150000	C	Montreal	C
P2	C	DB Develop.	C	Null	C	Null	C

Kiểm soát truy nhập phân tán

- Các vấn đề khác trong môi trường phân tán
  - Xác thực người dùng từ xa
    - Thường sử dụng dịch vụ thư mục
      - Nên nhân rộng tại một số trạm để sẵn sàng dùng
  - Quản lý các quy tắc Kiểm soát truy nhập tùy ý
    - Có vấn đề nếu nhóm người dùng trải rộng trên nhiều trạm
      - Quy tắc được lưu tại một số thư mục dựa theo vị trí nhóm người dùng
      - Việc truy nhập các quy tắc có thể phát sinh các truy vấn từ xa
  - Các kênh bí mật trong Kiểm soát truy nhập nhiều mức

Các kênh bí mật

- Phương tiện gián tiếp để truy nhập dữ liệu trái phép
- Ví dụ
  - Xem xét một CSDLPT với 2 trạm: C (Bảo mật) và S (Bí mật)
  - Tuân theo quy tắc "không ghi lại", một cập nhật từ một chủ thể với quyền Bí mật chỉ có thể được gửi tới S
  - Theo quy tắc "không đọc lên", một truy vấn đọc từ cùng một chủ thể có thể được gửi tới cả C và S
  - Nhưng truy vấn có thể chứa thông tin bí mật (ví dụ, trong một vị từ phép chọn), kênh bí mật tiềm năng cũng vậy.
- Giải pháp: nhân bản một phần CSDL
  - Như vậy, một trạm có mức bảo mật *L* chứa tất cả dữ liệu mà một chủ thể tại trạm mức *L* có thể truy nhập (ví dụ, *S* ở trên sẽ nhân bản dữ liệu bảo mật để nó có thể xử lý hoàn toàn các truy vấn bí mật).

31