Chương 7:
Thiết kế bảo mật cơ sở dữ liệu

Khoa Khoa học và Kỹ thuật Máy tính
Đại học Bách Khoa Tp.HCM

Nội dung

1. Giới thiệu thiết kế bảo mật cơ sở dữ liệu
2. Thiết kế hệ quản trị cơ sở dữ liệu an toàn
3. Thiết kế cơ sở dữ liệu an toàn

Thiết kế bảo mật cơ sở dữ liệu

- Gồm 2 cấp: thiết kế hệ quản trị cơ sở dữ liệu (Database Management System - DBMS) an toàn và thiết kế cơ sở dữ liệu (CSDL) an toàn.
- ***Thiết kế hệ quản trị CSDL an toàn (Secure DBMS design)***: để có được một CSDL an toàn thì trước hết phải có được một hệ quản trị CSDL an toàn. Có rất nhiều kiến trúc dựa trên những những thành phần khác nhau trong một hệ thống mà người dùng không thể tin tưởng hoàn toàn.
- ***Thiết kế CSDL an toàn (Secure database design)***: dựa theo một chính sách bảo mật có chọn lọc, được hiện thực và kiểm tra.

Nội dung

1. Giới thiệu thiết kế bảo mật cơ sở dữ liệu
2. Thiết kế hệ quản trị cơ sở dữ liệu an toàn
3. Thiết kế những cơ sở dữ liệu an toàn

Thiết kế hệ quản trị CSDL an toàn

- Cơ chế bảo mật
- Mô hình ủy quyền "System R"
- Kiến trúc hệ quản trị CSDL an toàn
- Các sản phẩm thương mại

Cơ chế bảo mật (Security mechanisms)

- Phải cung cấp cơ chế **điều khiển truy cập trên nhiều độ mịn dữ liệu khác nhau** (different degrees of granularity) như: lược đồ, quan hệ, cột, hàng, trường dữ liệu
- Phải cung cấp **nhiều chế độ truy cập** (different access modes) khác nhau như: SELECT, INSERT, UPDATE, DELETE
- Phải cung cấp **nhiều cơ chế điều khiển truy cập khác nhau** (different access control): phụ thuộc theo tên (name-dependent), phụ thuộc theo dữ liệu (data-dependent), và phụ thuộc theo ngữ cảnh (context-dependent)

Cơ chế bảo mật

- ***Ủy quyền động (dynamic authorization)***: quyền của một người dùng có thể bị thay đổi trong khi CSDL vẫn hoạt động.
- Không có kênh biến đổi (convert channel)
- ***Điều khiển suy luận (inference controls)***: hệ quản trị CSDL có cơ chế cho phép phân loại và bảo vệ các thông tin tổng hợp (aggregate information)
- Hỗ trợ cơ chế ***bảo vệ đa mức (multilevel protection)*** và ***tính đa thể hiện (polyinstantiation)*** thông qua các chính sách bắt buộc (mandatory policy)

Cơ chế bảo mật

- ***Cung cấp cơ chế kiểm toán***: các sự kiện liên quan đến vấn đề bảo mật cần được ghi nhận lại trong audit trail hoặc system log
- ***Không có cửa hậu (no backdoors):*** mọi truy cập vào dữ liệu phải thông qua hệ quản trị CSDL
- ***Hiệu suất tốn cho việc bảo mật ở mức hợp lý***

Thiết kế hệ quản trị CSDL an toàn

- Cơ chế bảo mật
- **Mô hình ủy quyền "System R"**
- Kiến trúc hệ quản trị CSDL an toàn
- Các sản phẩm thương mại

Mô hình ủy quyền "System R"

- Mô hình ủy quyền "System R" được định nghĩa bởi Griffiths và Wade (1976), và sau đó được chỉnh sửa lại bởi Fagin (1978).
- Do phòng nghiên cứu của IBM (IBM Research Laboratory) phát triển
- Đối tượng cần được bảo vệ: các bảng dữ liệu (base table/view)
- Các chế độ truy cập:
  - Read
  - Insert
  - Delete
  - Update
  - Drop

Mô hình ủy quyền "System R"

- Người tạo ra bảng nào thì có tất cả quyền trên bảng đó và có thể gán (GRANT) /thu hồi (REVOKE) quyền trên bảng đó.
- Phép gán GRANT được biểu diễn:

  <s, p, t, ts, g, go>

  - s: người được gán quyền (grantee)
  - p: quyền sẽ được gán granted.
  - t: quyền p có tác dụng trên bảng t
  - ts: timestamp của thao tác gán
  - g: người thực hiện gán quyền (grantor).
  - go $\in$ {yes , no}: grant option.

Phép gán GRANT

- Phép gán GRANT được biểu diễn:

  <s, p, t, ts, g, go>

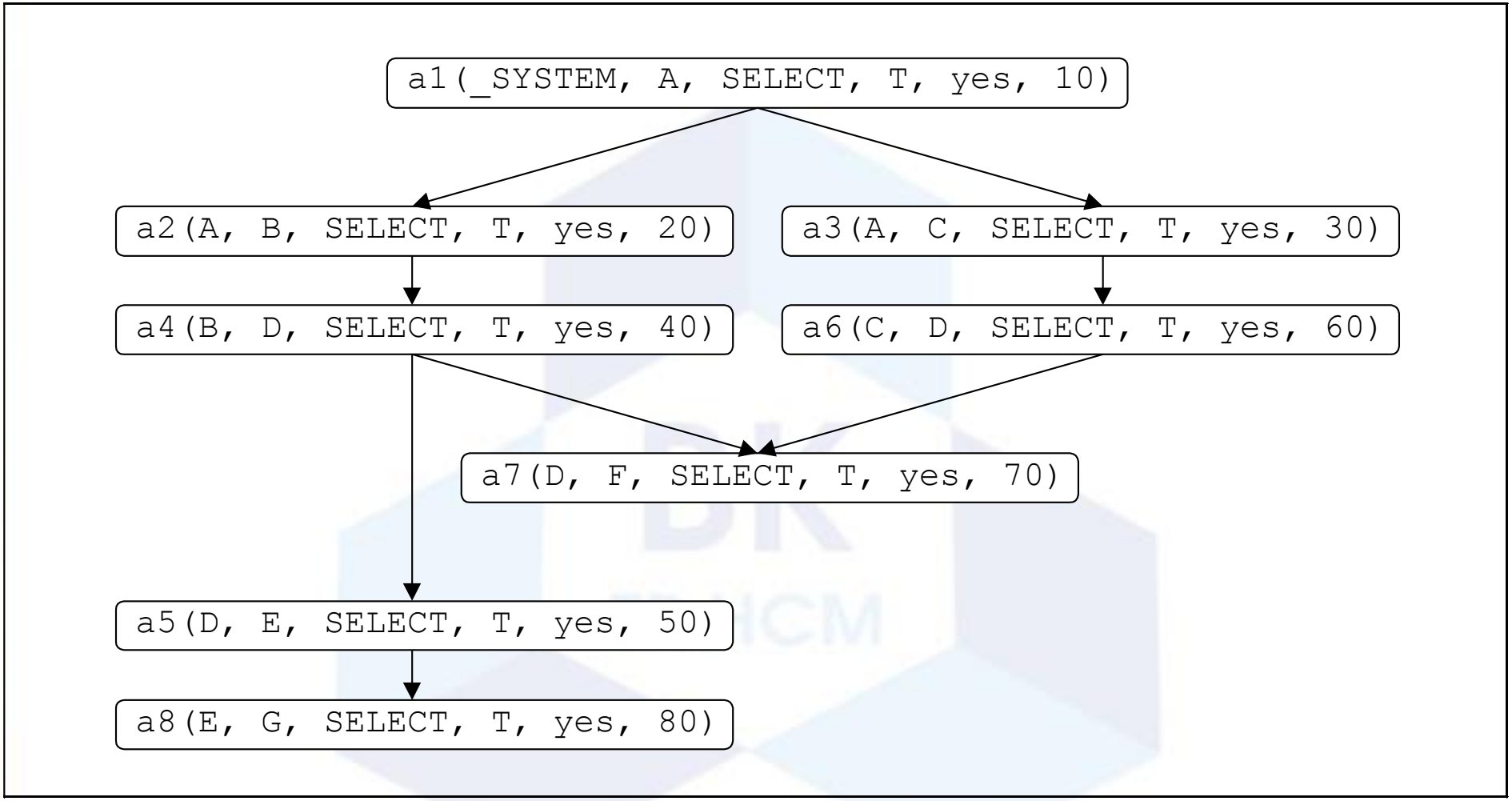
- Ví dụ:
  - <B, select, T, 10, A, yes>
  - <C, select, T, 20, B, no>

Cú pháp GRANT và REVOKE

- Câu lệnh GRANT và REVOKE trong SQL

GRANT { ALL RIGHTS | ⟨privileges⟩ | ALL BUT ⟨privileges⟩ } ON ⟨table⟩ TO ⟨user-list⟩ [WITH GRANT OPTION]

REVOKE { ALL RIGHTS ON | ⟨privileges⟩ ON } ⟨table⟩ FROM ⟨user-list⟩

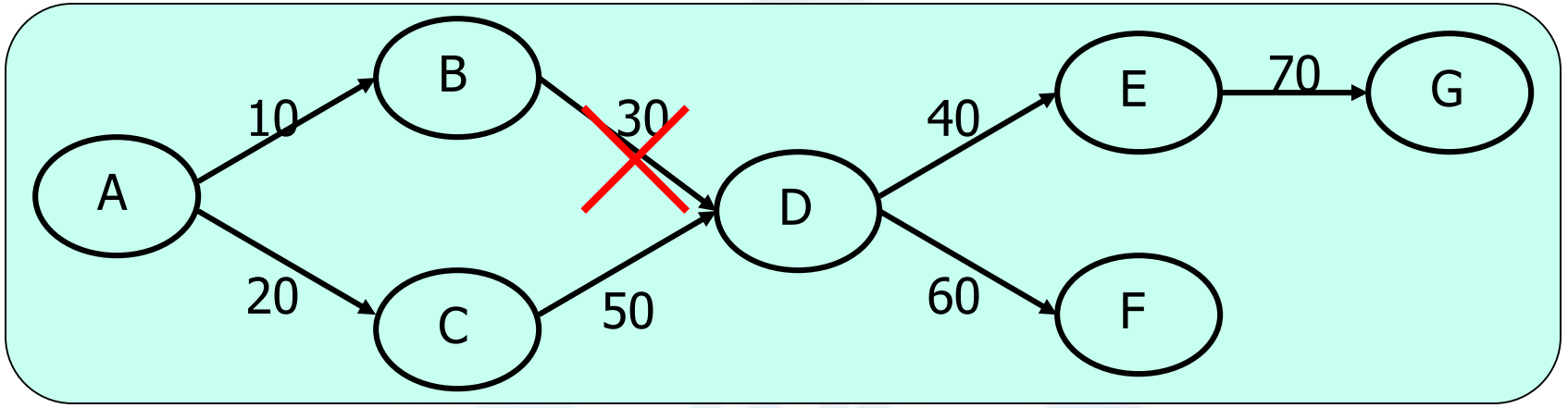

a1(_SYSTEM, A, SELECT, T, yes, 10)
a2(A, B, SELECT, T, yes, 20)
a3(A, C, SELECT, T, yes, 30)
a4(B, D, SELECT, T, yes, 40)
a6(C, D, SELECT, T, yes, 60)
a7(D, F, SELECT, T, yes, 70)
a5(D, E, SELECT, T, yes, 50)
a8(E, G, SELECT, T, yes, 80)

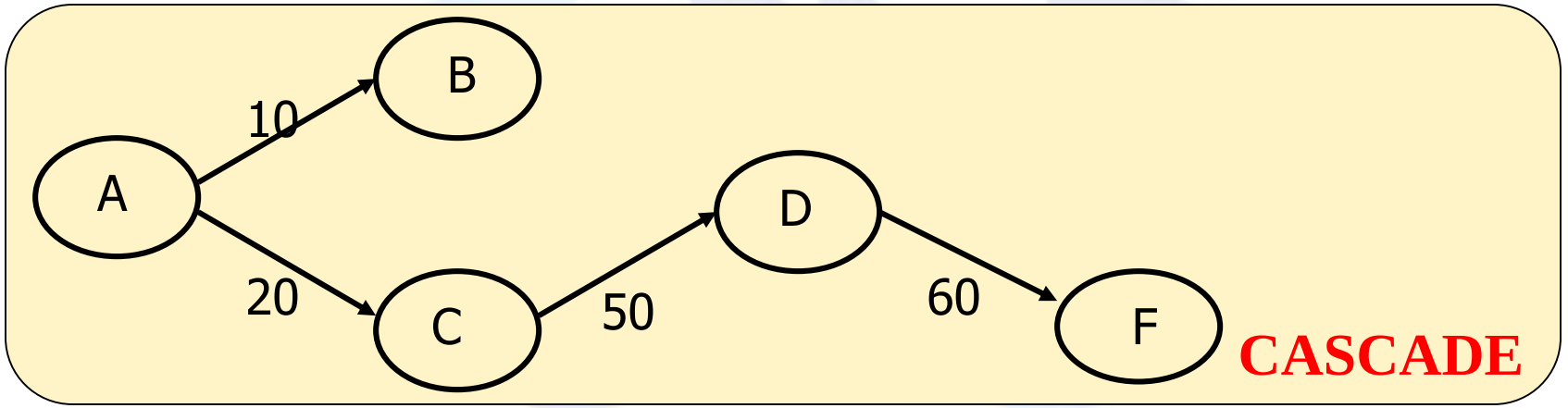
Quá trình thu hồi quyền (Revocation)

- Quá trình thu hồi quyền (Revocation)
  - Người dùng chỉ có thể thu hồi lại những quyền do chính mình gán cho người dùng khác.
  - Không thể chỉ thu hồi GRANT OPTION
- Có 3 cách thu hồi quyền
  - Thu hồi quyền đệ quy (recursive/cascade) dựa trên timestamp
  - Thu hồi quyền không đệ quy
  - Thu hồi quyền không đệ quy mở rộng

Quá trình thu hồi quyền (Revocation)

- Quá trình thu hồi quyền đệ quy dựa trên timestamp





Quá trình thu hồi quyền (Revocation)

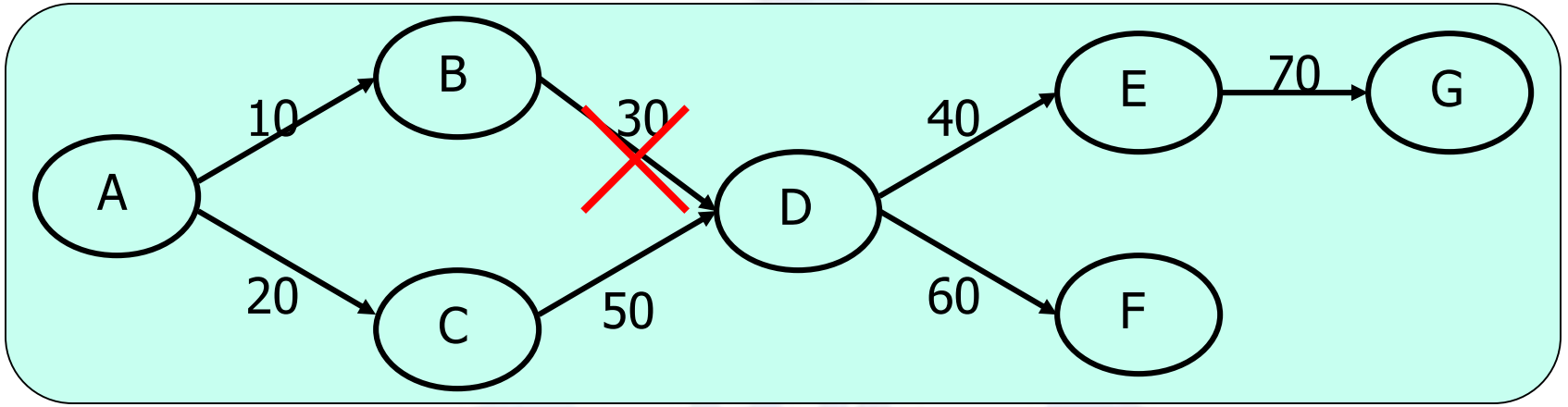
- **Thu hồi quyền đệ quy (recursive/cascade)** dựa trên timestamp có thể là một thao tác gây hại cho hệ thống
- Thu hồi quyền đệ quy (recursive/cascade) dựa trên timestamp dẫn đến
  - Thu hồi kéo theo toàn bộ những quyền do người dùng bị thu hồi gán cho người khác

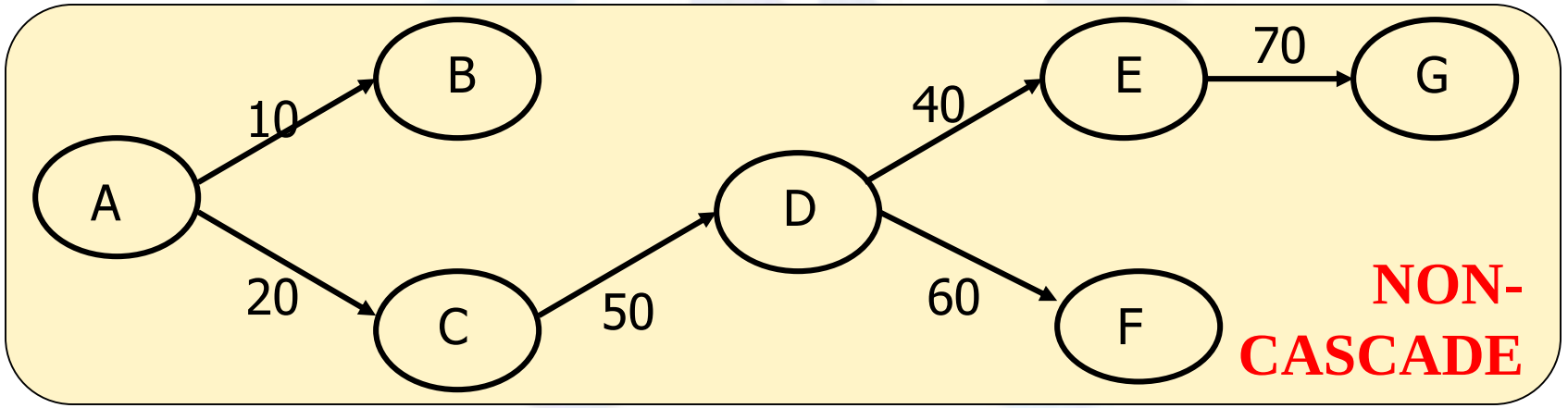
    → Không hỗ trợ quyền cho người dùng cần thiết

    → Gây ra lỗi cho các chương trình và view

Quá trình thu hồi quyền (Revocation)

- Quá trình thu hồi quyền không đệ quy



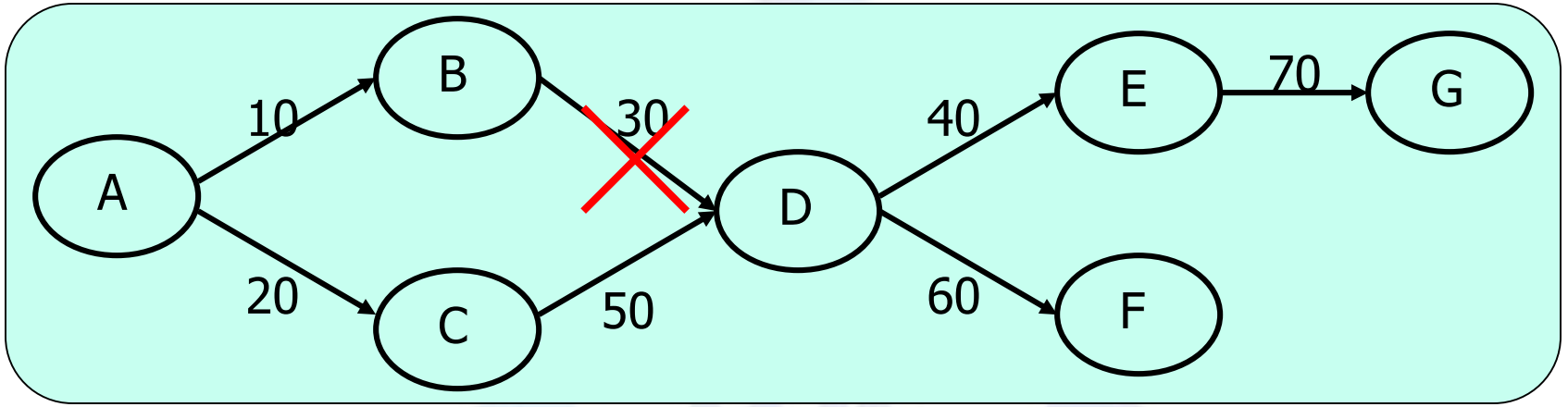


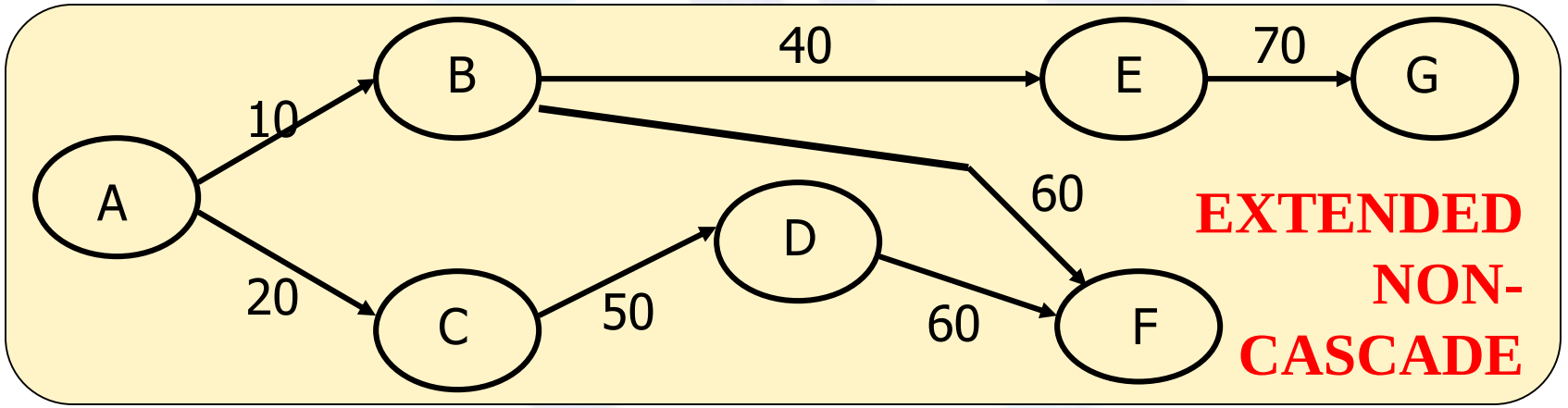
Quá trình thu hồi quyền (Revocation)

- **Thu hồi quyền không đệ quy**
  - Không tự động thu hồi lại những quyền của những người dùng khác được gán bởi người dùng đã bị thu hồi quyền
    → Mất kiểm soát các quyền
- **Thu hồi quyền không đệ quy mở rộng**
  - Vẫn giữ các quyền của những người dùng khác được gán bởi người dùng đã bị thu hồi quyền nhưng điều chỉnh lại thông tin người gán của những người dùng này thành người dùng thu hồi quyền

Quá trình thu hồi quyền (Revocation)

- Quá trình thu hồi quyền không đệ quy mở rộng





Mô hình ủy quyền "System R"

- View
  - Là cơ chế điều khiển truy cập dựa trên nội dung
  - Người tạo view có quyền xóa (drop) view nhưng không có tất cả các quyền trên view (phụ thuộc bảng nền)
  - Người tạo view có những quyền giống với quyền trên bảng nền.
  - Người tạo view (nếu có GRANT OPTION trên bảng nền) có thể gán quyền trên view cho những người dùng khác.
  - Sau khi người dùng tạo view, những quyền trên bảng nền được gán cho người dùng sẽ không được thêm vào view.
  - Những quyền bị thu hồi trên bảng cơ sở cũng sẽ bị thu hồi trên view

Hiện thực mô hình "System R"

- Thông tin về quyền của các người dùng được lưu trong bảng
  - SYSAUTH
  - SYSCOLAUTH
- **SYSAUTH:**
  - Userid: mã người dùng
  - Tname: tên bảng
  - Grantor: người gán
  - Type: loại của Tname, là "R" (là relation) hoặc "V" (là view)
  - Các cột Read / Insert / Delete / Update: thời điểm được gán
  - Grantopt: "yes" hoặc "no"

Hiện thực mô hình "System R"

- **SYSAUTH:**

Userid	Tname	Type	Grantor	Read	Insert	Delete	Update	Grantopt
B	Emp	R	A	10	0	0	0	yes
C	Emp	R	A	20	0	0	0	yes
D	Emp	R	B	30	0	0	0	yes
E	Emp	R	D	40	0	0	0	yes
D	Emp	R	C	50	0	0	0	yes
F	Emp	R	D	60	0	0	0	yes
G	Emp	R	E	70	0	0	0	yes

Hiện thực mô hình "System R"

- **SYSCOLAUTH:** lưu thông tin về các cột được phép UPDATE của người dùng
  - Userid: mã người dùng
  - Table: tên bảng
  - Column: cột được phép UPDATE
  - Grantor: người gán
  - Grantopt: "yes" hoặc "no"

Mô hình ủy quyền "System R" mở rộng

- **Nhóm người dùng (group):** Giảm công sức khi phân phối các quyền. Người dùng trong các nhóm có thể trùng lắp nhau (overlap)
- **Quá trình thu hồi quyền không đệ quy mở rộng**
- **Ủy quyền phủ định (negative authorizations):** người dùng có thể định nghĩa một quyền phủ định ngăn không cho một người dùng khác truy cập vào bảng của mình

Thiết kế hệ quản trị CSDL an toàn

- Cơ chế an toàn
- Mô hình ủy quyền "System R"
- **Kiến trúc hệ quản trị CSDL an toàn**
- Các sản phẩm thương mại

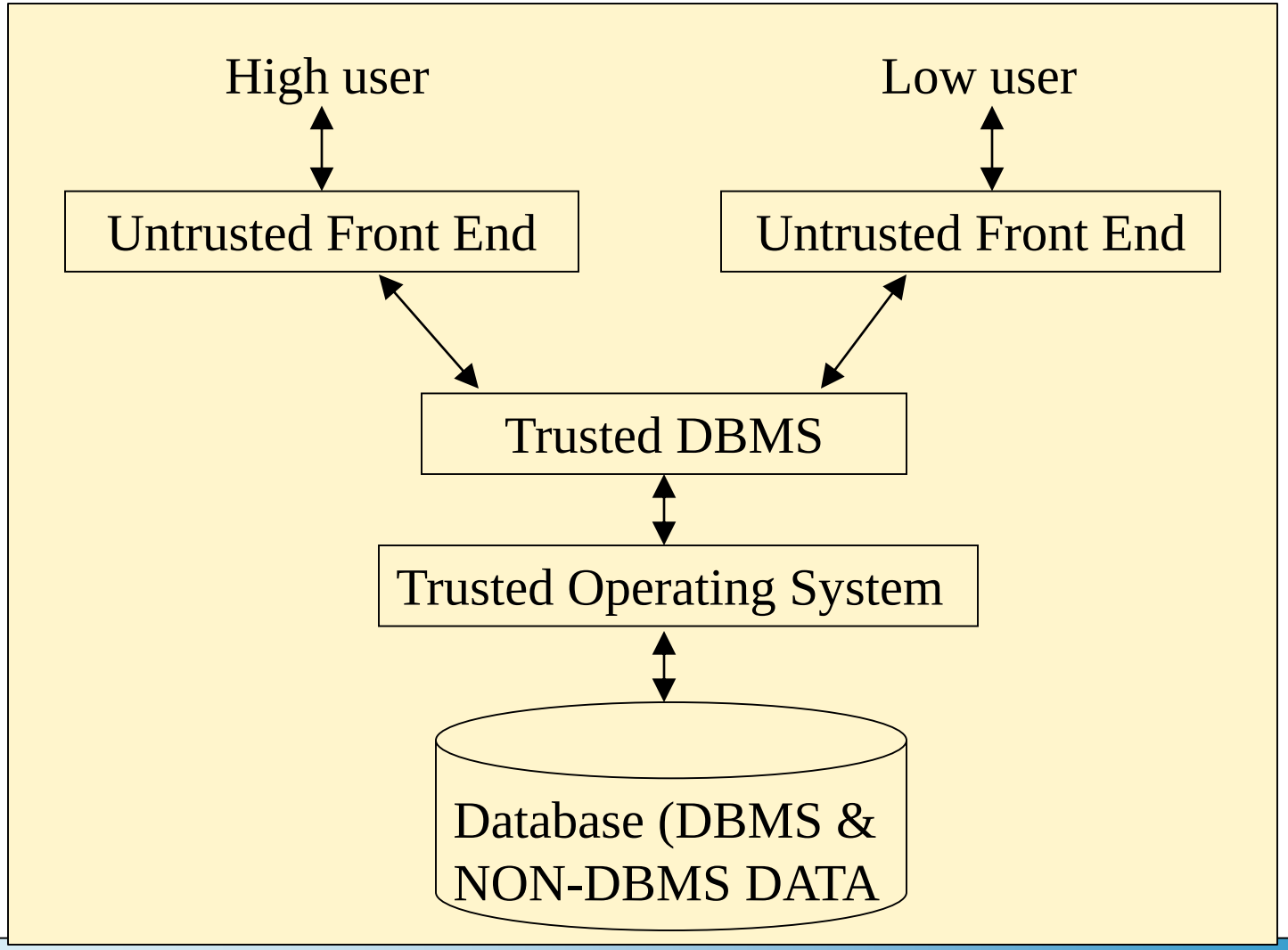
Kiến trúc hệ quản trị CSDL an toàn

- Có 2 chế độ:
  - Chế độ "hệ thống cao" ("System high" mode)
  - Chế độ đa mức (Multilevel mode): có các kiến trúc
    - Trusted subject
    - Woods Hole: Integrity lock, Kernelized, Replicated

"System high" mode

- Tất cả các người dùng đều ở mức bảo mật cao nhất
- Người dùng phải xem xét lại tất cả dữ liệu trước khi đưa ra sử dụng.
- Bảo mật thấp do phụ thuộc con người

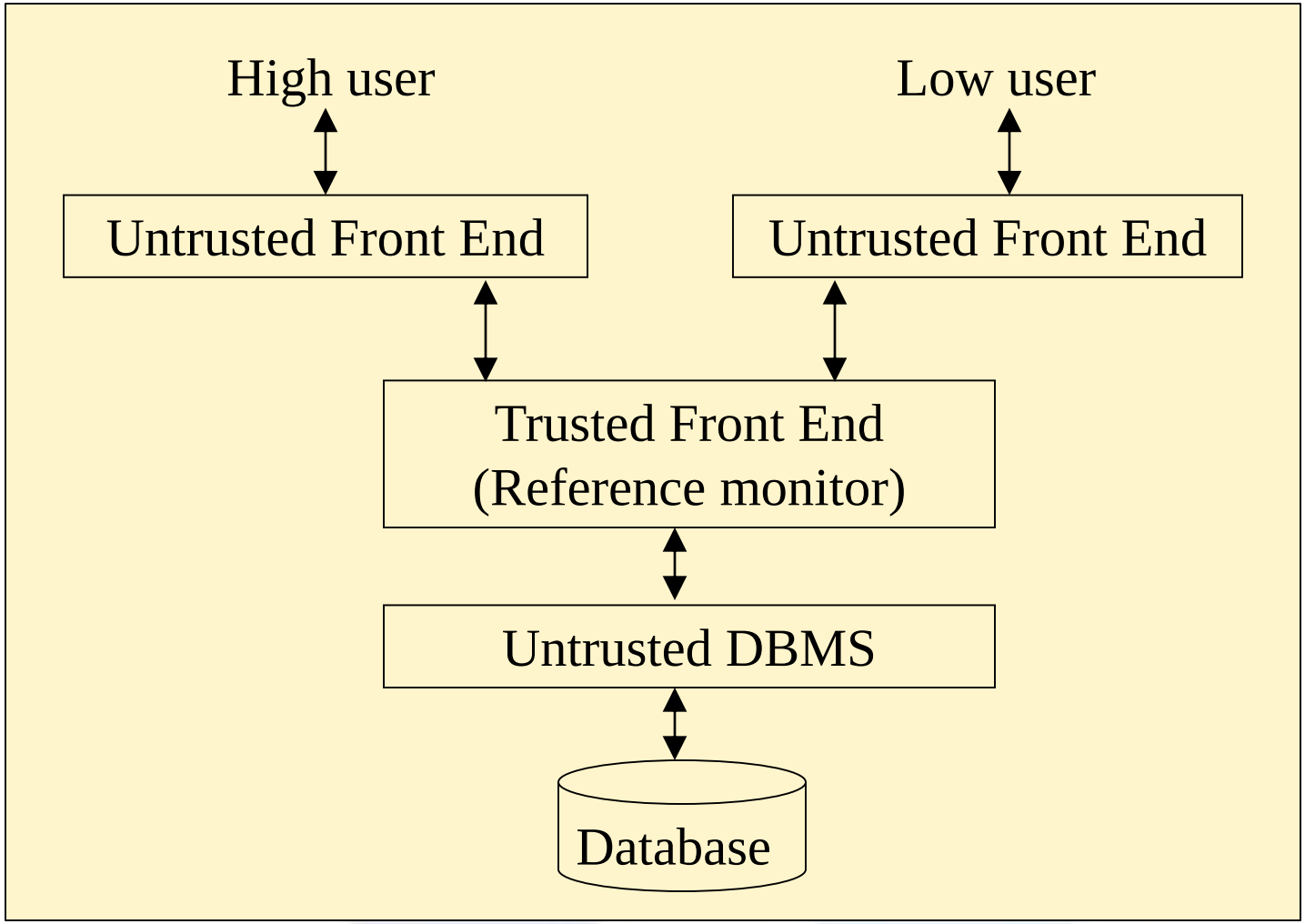
Multilevel mode - Trusted subject Architecture



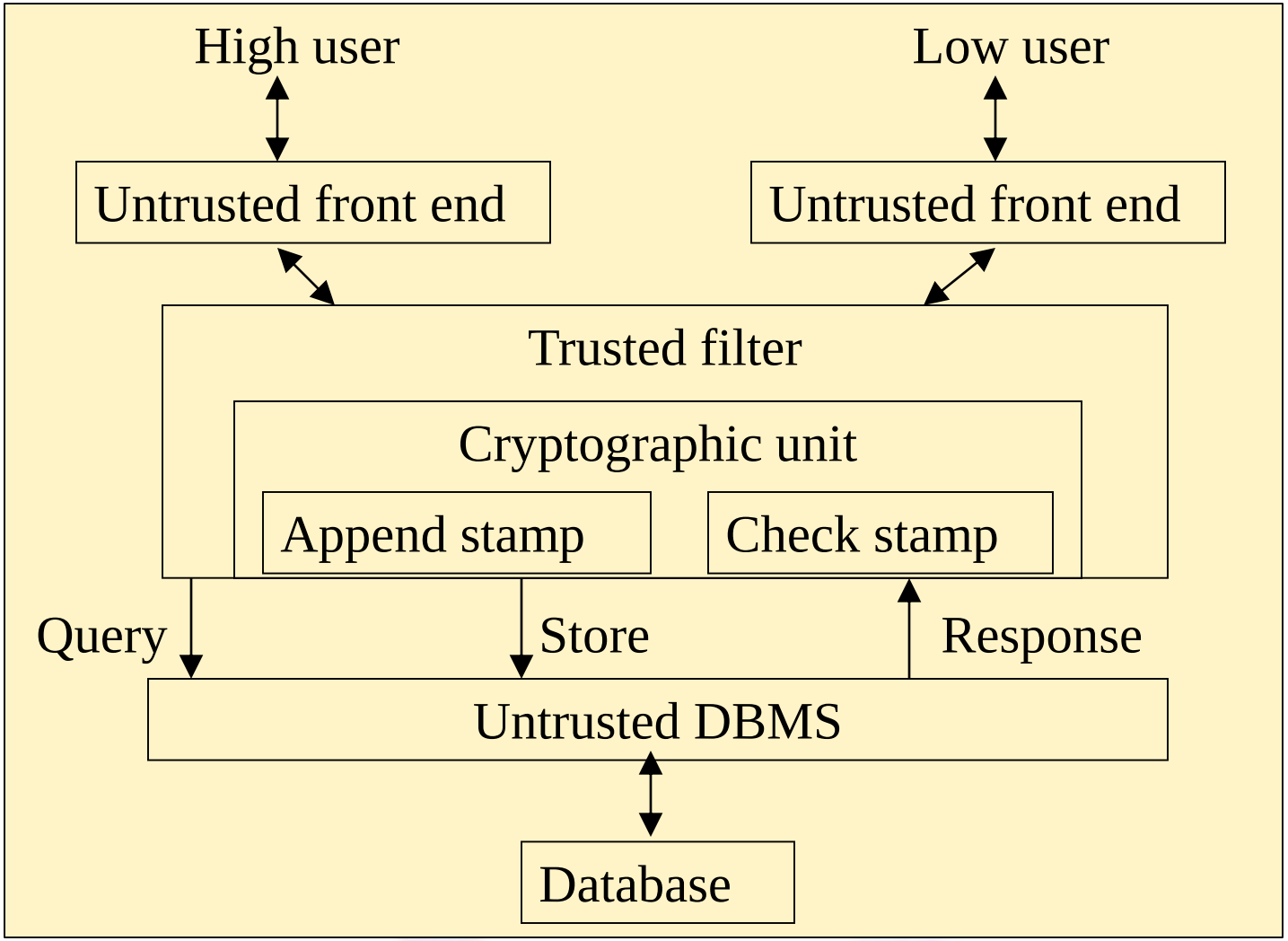
Multilevel mode - Trusted subject Architecture

- Mỗi chủ thể mang nhãn bảo mật của DBMS được xem là chủ thể đáng tin cậy và được cho qua các điều khiển bắt buộc của hệ điều hành
- Sybase là hệ quản trị CSDL theo kiến trúc này
- Ưu điểm
  - Bảo mật cao
  - Ít tốn chi phí (overhead) trong thao tác truy xuất và cập nhật
- Khuyết điểm
  - Cần nhiều đoạn code đáng tin cậy

Multilevel mode - Woods Hole



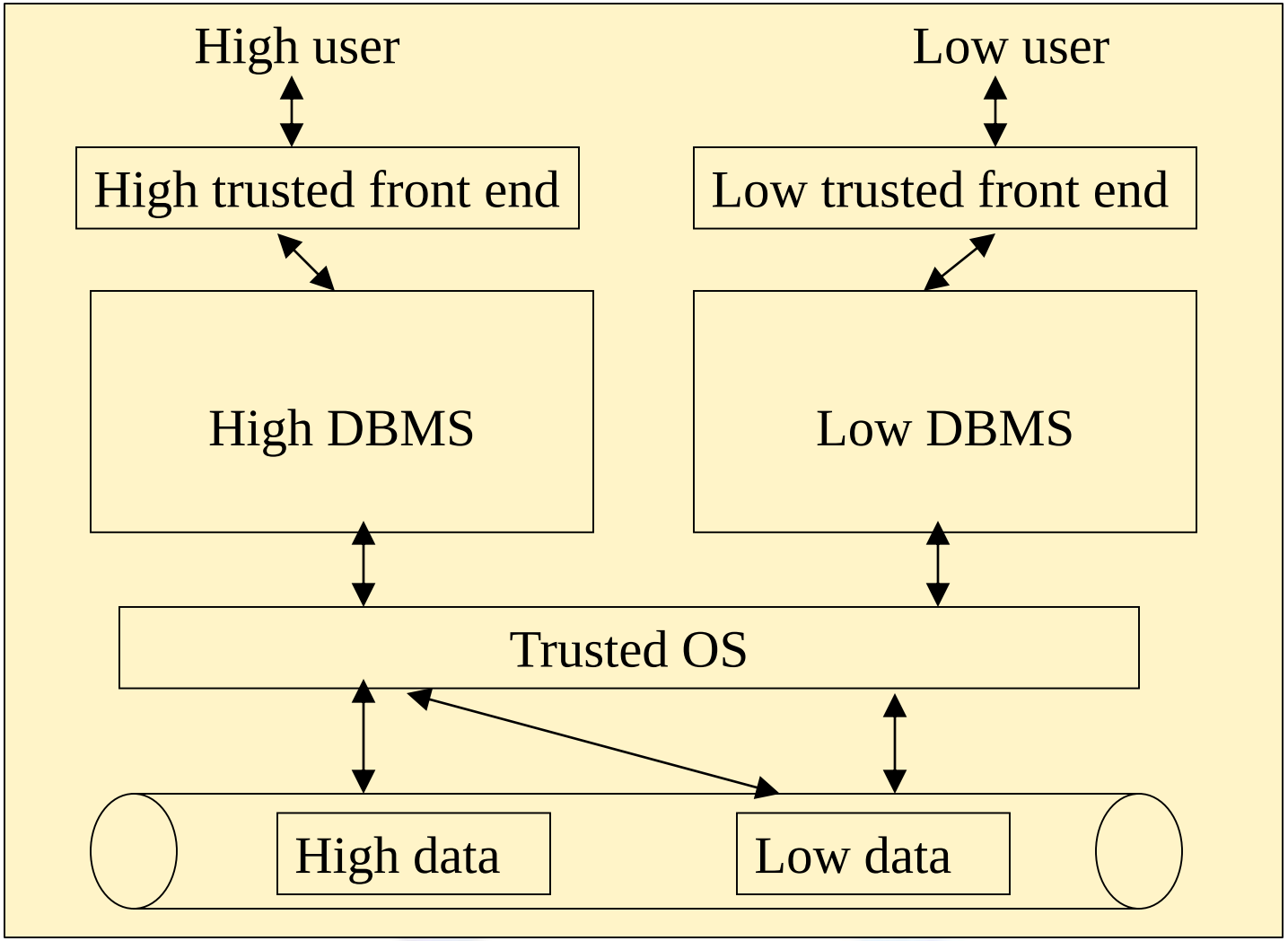
Multilevel mode - Integrity lock



Multilevel mode - Integrity lock

- Một bộ lọc tin cậy (trusted filter) chịu trách nhiệm bảo vệ các đối tượng dữ liệu theo cơ chế đa mức bằng cách tạo vào gán các nhãn bảo mật, được gọi là tem (stamp).
- TRUDATA là DBMS theo kiến trúc này
- Ưu điểm
  - Phát hiện ra những thay đổi bất hợp pháp
  - Chống Trojan Horses
  - Sử dụng được ở những DBMS không tin cậy
- Khuyết điểm
  - Cần quản lý các khóa
  - Mối nguy hiểm suy luận (Inference threat)

Multilevel mode - Kernelized



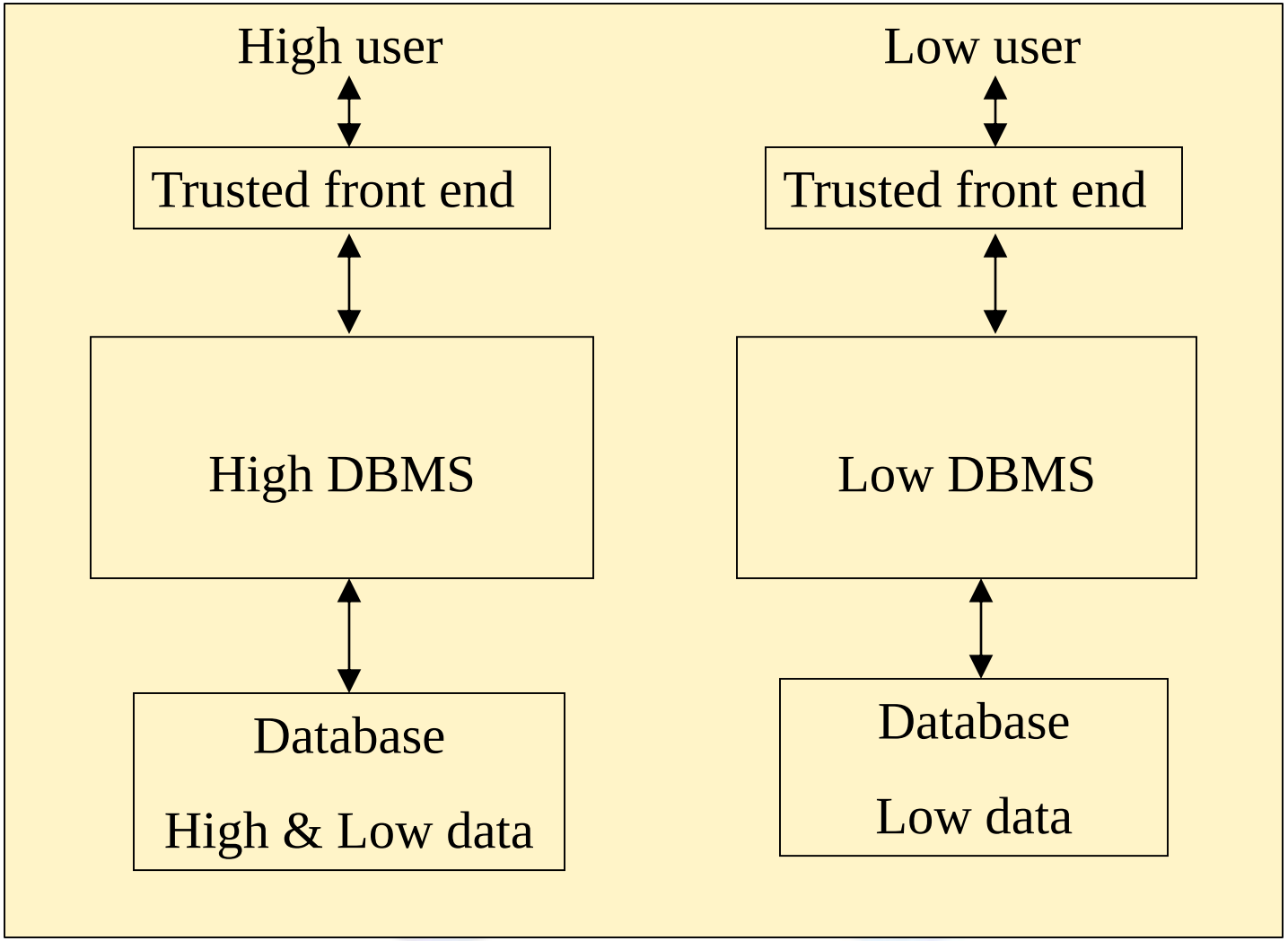
Multilevel mode - Kernelized

- Hệ điều hành tin cậy sẽ chịu trách nhiệm điều khiển truy cập ở cấp vật lý cho dữ liệu trong CSDL bằng cơ chế bảo vệ bắt buộc (mandatory protection)
- Phân rã: một quan hệ đa mức thành nhiều quan hệ một mức
- Phục hồi: sinh ra các view đa mức
- Prototype SeaView (1988) và DBMS Oracle theo kiến trúc này

Multilevel mode - Kernelized

- Ưu điểm:
  - Dễ hiện thực
  - Mức độ an toàn cao
- Khuyết điểm
  - Tốn thêm chi phí (overhead)
    - Hệ điều hành chịu thêm trách nhiệm bảo mật dữ liệu theo nhiều mức
  - Cần phải kết nối dữ liệu từ nhiều mức khác nhau của CSDL
    - Khi thực hiện câu truy vấn của người dùng tin cậy cấp cao

Multilevel mode - Replicated



Multilevel mode - Replicated

- Dữ liệu cấp thấp được sao chép lại (replicated)
- Kiến trúc này chưa có DBMS thương mại, chỉ có bản prototype NRL
- Ưu điểm:
  - Dễ truy cập
- Khuyết điểm:
  - Cần giải thuật đồng bộ
  - Chi phí đắt

Thiết kế hệ quản trị CSDL an toàn

- Cơ chế an toàn
- Mô hình ủy quyền "System R"
- Kiến trúc hệ quản trị CSDL an toàn
- **Các sản phẩm thương mại**

Các sản phẩm thương mại

- Sybase secure server
- Ingres
- Oracle
- DB2

Các sản phẩm thương mại - Sybase secure server

- Đối tượng:
  - Đối tượng chính (primary object): hàng, đây là đối tượng nhỏ nhất có thể đánh nhãn bảo mật
  - Đối tượng thứ cấp (secondary objects): bảng, CSDL
- Chủ thể: người dùng và nhóm người dùng
- Điều khiển truy cập:
  - Kiểm tra quyền của người dùng dựa vào các nhãn bảo mật
  - Table: MAC, DAC
  - View: DAC, MAC
- Cho phép cấu hình cho Audit

Các sản phẩm thương mại - Ingres

- Chủ thể là người dùng và nhóm người dùng
- Khi chạy một ứng dụng, người dùng phải nhập role và password của role đó
- Đối tượng: CSDL, catalogues, tables, views, procedures.
- Có lệnh GRANT nhưng không có Grant Option.
- Câu lệnh Auditdb dùng để audit

Các sản phẩm thương mại - Oracle

- Các chủ thể có thể được tạo ra, thay đổi hoặc xóa đi
- Gán role cho một role khác sẽ tạo ra hệ thống cấp bậc
- Các tài khoản đặc biệt:
  - Sys, System -> DBA privilege.
  - Public -> nhóm các người dùng cơ bản
- Đối tượng: databases, tables, views
- Thao tác:
  - Bảng: Select, Insert, Update, Delete, Alter, Index, Reference
  - View: Select, Insert, Update and Delete
  - Procedure: Execute
  - Có **Grant option**

Các sản phẩm thương mại – DB2

- Đối tượng: tables, system catalogue
- Bảng quản lý quyền: Systables và Syscolumns

Nội dung

1. Giới thiệu thiết kế bảo mật cơ sở dữ liệu
2. Thiết kế hệ quản trị cơ sở dữ liệu an toàn
3. Thiết kế những cơ sở dữ liệu an toàn

Bảo mật cơ sở dữ liệu

- **Bảo mật cơ sở dữ liệu (database security):** là 1 hệ thống, quy trình hay 1 thủ tục để bảo vệ cơ sở dữ liệu khỏi các tác động ngoài ý muốn: lạm dụng quyền hạn, vô ý hoặc cố ý trong truy cập cơ sở dữ liệu.
- Các cơ chế bảo mật CSDL:
  - Xác thực (Authentication)
  - Điều khiển truy cập (Acess control)
  - Điều khiển toàn vẹn (Integrity controls)
  - Kiểm toán (Auditing)
  - Mã hóa (Encryption)

Bảo mật cơ sở dữ liệu

- Mã hóa:
  - Mức tập tin: không cung cấp mức độ bảo mật truy cập đến CSDL ở mức bảng, cột, dòng. Không phân quyền cho người sử dụng
  - Mức ứng dụng: cho phép phân quyền, nhưng đòi hỏi sự thay đổi kiến trúc của ứng dụng thậm chí đòi hỏi ứng dụng phải viết lại
- Bảng ảo: tốc độ thực thi giảm.
- DBMS: giảm bớt sự rườm rà, nhất quán, dữ liệu được chia sẻ, tăng cường bảo mật, toàn vẹn dữ liệu

Thiết kế CSDL an toàn

- Thiết kế CSDL an toàn gồm các bước sau:
  - Phân tích sơ bộ: nghiên cứu tính khả thi
  - Xây dựng các yêu cầu và chính sách bảo mật: xác định những yêu cầu bảo mật cho các mối đe dọa.
  - Thiết kế ý niệm
  - Thiết kế luận lý
  - Thiết kế vật lý
  - Hiện thực
  - Kiểm tra

Phân tích sơ bộ

- ***Các mối đe dọa đến hệ thống:***
  - Mối đe dọa: được xác định khi có người (nhóm người) sử dụng các kỹ thuật đặc biệt để xem, sửa đổi trái phép các thông tin do hệ thống quản lý.
  - Tìm hiểu các cách thức tấn công, hậu quả.
- ***Các đặc tính của môi trường CSDL:*** Những ảnh hưởng của yêu cầu bảo mật đối với người dùng và các cơ chế liên quan.
  - Ví dụ: Hệ thống bảo vệ đa mức (Mutilevel protection system): chỉ phù hợp với môi trường quân đội, nhưng không thích hợp trong môi trường thương mại ...

Phân tích sơ bộ

- ***Khả năng áp dụng các sản phẩm bảo mật hiện có:***
  - Cân nhắc giữa việc sử dụng các sản phẩm thương mại hiện có với việc phát triển một hệ thống bảo mật từ đầu
  - Phụ thuộc vào hình thức, mức độ bảo mật và cả việc bảo mật được xem như là tính năng vốn có của cơ sở dữ liệu hay chỉ là một tính năng bổ sung
- ***Khả năng tích hợp của các sản phẩm bảo mật:*** tính khả thi của sản phẩm
  - Xem xét khả năng đáp ứng của phần cứng, phần mềm hiện có, khả năng nâng cấp....
  - Con người.

Phân tích sơ bộ

- ***Hiệu suất của hệ thống sau được bảo mật*:** so sánh hiệu suất của hệ thống mới xây dựng so với hệ thống đã tồn tại hoặc hệ thống không có các cơ chế bỏa mật.

Phân tích các yêu cầu

- ***Xem xét các nguy cơ của hệ thống***, giúp cho các designer xác định yêu cầu bảo mật một cách đúng đắn và đầy đủ.
- ***Phân loại hệ thống rủi ro cao hay thấp***: mức độ tương quan dữ liệu, chia sẻ dữ liệu, truy xuất dữ liệu, kỹ thuật được lựa chọn,...
- Gồm các bước:
  - Phân tích mức độ nhạy cảm của dữ liệu
  - Xác định các mối đe dọa và phân tích các lỗ hổng
  - Phân tích và đánh giá độ rủi ro
  - Định nghĩa các yêu cầu

Lựa chọn chính sách bảo mật

- Phải cân bằng giữa 3 tính chất sau tùy theo môi trường sử dụng:
  - Tính bảo mật
  - Tính toàn vẹn
  - Tính tin cậy

  Ví dụ: Tính bảo mật là cực kỳ quan trọng trong quân đội, nhưng trong thương mại thì tính toàn vẹn và độ tin cậy của dữ liệu quan trọng hơn.
- Nguyên tắc: Chia sẻ tối đa và quyền tối thiểu

Lựa chọn chính sách bảo mật

- ***Độ mịn của điều khiển (Granularity of control)***: phạm vi kiểm soát, kiểm soát như thế nào.
- ***Các thuộc tính dùng trong điều khiển truy cập:*** lớp đối tượng, thời gian, trạng thái của hệ thống, lịch sử truy cập.
- ***Độ ưu tiên****:* giải quyết các xung đột phát sinh giữa các chính sách bảo mật.

Lựa chọn chính sách bảo mật

- ***Quyền:*** xác định ai có thể trao quyền hoặc hủy bỏ quyền truy cập.
  - Ví dụ: quản lý tập trung hay phi tập trung. MAC, DAC, ...
- ***Phân quyền:*** phân nhóm người dùng, xác định các role và trách nhiệm của mỗi nhóm đối với hệ thống.
  - Ví dụ: các hệ thống đa mức, ...
- ***Tính thừa kế***: truyền quyền cho bản sao, hay dẫn xuất (instance) của đối tượng.

Thiết kế ý niệm

- Thiết kế phải xác định:
  - Chủ thể, đối tượng và vai trò của nó trong hệ thống.
  - Các chế độ truy cập được cấp cho các chủ thể khác nhau trên các đối tượng khác nhau, nhận dạng các ràng buộc truy cập .
  - Các quyền truy cập có thể chuyển cho ai và chuyển như thế nào (grant/ revoke) .
- Yêu cầu:
  - Đủ (complete): Thể hiện tất cả các yêu cầu bảo mật đã đặt ra
  - Nhất quán (consistent): tránh hiện tượng không nhất quán trong truy xuất đến 1 đối tượng.

Thiết kế luận lý

- Lựa chọn 1 DBMS:
  - Chi phí mua phần mềm
  - Chi phí mua phần cứng
  - Chi phí bảo trì
  - Chi phí tạo và chuyển đổi CSDL
  - Chi phí con người
  - Chi phí đào tạo
  - Chi phí vận hành

Thiết kế luận lý

- Dịch mô hình ý niệm thành những mô hình dữ liệu theo DBMS được chọn.
  - Lập bảng: không xem xét các đặc điểm cụ thể hay các trường hợp đặc biệt.
  - Kết nối các bảng với nhau.

Thiết kế vật lý

- Tổ chức, lưu trữ, hiện thực và tích hợp các cơ chế bảo mật.
- Phụ thuộc:
  - Thời gian đáp ứng
  - Không gian lưu trữ
  - Số thao tác trên 1 đơn vị thời gian

Hiện thực các cơ chế bảo mật

- ***Tiết kiệm:*** Lựa chọn phương thức đơn giản, hiện thực đơn giản, giảm lỗi, giảm chi phí, dễ kiểm tra kiểm thử.
- ***Hiệu quả:*** thời gian chạy, hiệu suất, quá tải.
- ***Chi phí tuyến tính:*** chi phí cũng cần được xem xét trong lựa chọn phương thức.
- ***Tách quyền:*** phân lớp các phương thức, định ra điều kiện truy cập, sử dụng nhiều lớp password.

Hiện thực các cơ chế bảo mật

- ***Quyền tối thiểu***: hạn chế rủi ro, dễ dàng bảo trì, ngăn chặn Trojan,
- ***Kiểm soát đầy đủ***: mỗi truy xuất đều phải được kiểm tra.
- Lựa chọn các ***kỹ thuật đã được kiểm tra và đáng tin cậy.***
- ***Bảo mật mặc định:*** áp dụng trong trường hợp người sử dụng không định nghĩa.
- ***Cơ chế chung tối thiểu***: các phương thức nên hoạt động 1 cách độc lập.

Hiện thực các cơ chế bảo mật

- ***Dễ sử dụng*** giúp người dùng sử dụng đúng.
- ***Tính uyển chuyển, linh động:*** cơ chế phải hoạt động ngay cả trong những điều kiện xấu nhất có thể.
- ***Sự độc lập:*** chia nhỏ hệ thống tránh bị giả mạo.
- ***Có thể chứng minh:*** phải đáp ứng các yêu cầu đã đặt ra, phải chứng minh là nó hoạt động chính xác.

Hiện thực các cơ chế bảo mật

- ***Tính đủ và nhất quán:*** tuân thủ nghiêm ngặt các quy tắc kỹ thuật mà thiết kế mô tả.
- Tìm hiểu các ***cách thức tấn công và cách đề phòng.***
- ***Xóa những dữ liệu còn sót lại*** trong bộ nhớ trước khi sử dụng lại bộ nhớ.
- ***Tính vô hình của dữ liệu:*** không để người dùng thấy được thông tin về cấu trúc cũng như sự tồn tại của đối tượng mà họ không được phép truy cập (tên đối tượng,...).

Hiện thực các cơ chế bảo mật

- ***Các khả năng phá hỏng hệ thống (work factor)***
- ***Bẫy cố ý:*** đăt bẫy giúp dễ phát hiện những nỗ lực phá vỡ hệ thống.
- ***Cách xử lý khẩn cấp:*** cung cấp cho những người đáng tin cậy khả năng vô hiệu hóa những phương thức đặc biệt.
- ***Phần cứng phải đáng tin cậy*** vì lỗi phần cứng có thể bị lợi dụng để tấn công, có cơ chế lưu và khôi phục dữ liệu.
- ***Ngôn ngữ lập trình***: lựa chọn ngôn ngữ lập trình và sử dụng lập trình viên có kỹ năng lập trình tốt để làm giảm tỉ lệ lỗi.

Kiểm tra

- ***Mục đích:*** kiểm tra các phần mềm và các chính sách an toàn
- Được thực hiện thông qua sản phẩm phần mềm và cần có sẵn các phương pháp hình thức và phi hình thức, dựa vào hoặc không dựa vào các kí hiệu toán học
- Các phương pháp phi hình thức dựa trên
  - Kiểm soát chéo các yêu cầu/ chương trình nguồn, hoặc các yêu cầu/các hành vi tại thời gian chạy
  - Duyệt lại chương trình phần mềm để phát hiện ra các lỗi/ các mâu thuẫn (tính không nhất quán)

Kiểm tra

- Các phương pháp phi hình thức dựa trên
  - Phân tích hành vi của chương trình, tùy thuộc vào các tham số khác nhau, nhằm kiểm tra các đường dẫn thực hiện khác nhau và các biến thể tương ứng của các tham số
  - Thông qua thử nghiệm, gỡ rối

    ➔ Áp dụng một cách nhanh chóng, không cần định nghĩa trước mô hình an toàn hình thức. Có thể xác định hành vi của phần mềm trong các trường hợp cụ thể, nhưng nó không thể chỉ ra các hoạt động trái phép trong hệ thống

Kiểm tra

- Các phương pháp hình thức tinh xảo hơn, chúng dựa vào các kí hiệu và các phương pháp toán học.
- Các đặc tả hình thức mức cao tinh xảo hơn các đặc tả mức trung gian và các đặc tả mức thấp
- Các kỹ thuật này có thể chứng minh mô hình là cơ chế an toàn, thông qua việc chứng minh tính đúng đắn của các đặc tả hình thức

Hậu quả của quy hoạch và thiết kế CSDL sơ sài

- Đối tượng chính bị loại bỏ
- Chứa quá nhiều hay quá ít thông tin
- CSDL không chỉnh sửa dễ dàng theo nhu cầu
- Hướng dẫn hạn chế hoặc không có hướng dẫn sử dụng cho người dùng
- Phân bổ tài nguyên (thời gian, tiền bạc) không tốt, quá trình thi công bị gián đoạn do thay đổi nhân sự,...

Nội dung

1. Giới thiệu thiết kế bảo mật cơ sở dữ liệu
2. Thiết kế hệ quản trị cơ sở dữ liệu an toàn
3. Thiết kế những cơ sở dữ liệu an toàn


Question ?