Buổi 7

CÁC MÔ HÌNH, CHÍNH SÁCH AN TOÀN BẮT BUỘC (MAC)

Giới thiệu chung

- Chính sách an toàn bắt buộc sẽ đảm bảo an toàn cho hệ thống ở mức độ cao hơn so với chính sách an toàn tuỳ ý, bởi vì ngoài việc kiểm soát quyền truy nhập vào dữ liệu thì chính sách an toàn bắt buộc còn kiểm soát luồng dữ liệu

- Một số mô hình an toàn bắt buộc: mô hình Bell - Lapadula(1973,1974,1975), mô hình Biba (1977), mô hình Sea View, Dion,…

- MAC:

+ Được áp dụng cho các thông tin có yêu cầu bảo vệ nghiêm ngặt

+ Hạn chế truy nhập của các chủ thể vào các đối tượng bằng cách sử dụng các nhãn an toàn (label)

MAC (MANDATORY ACCESS CONTROL)

- Mọi chủ thể và đối tượng trong hệ thống đều được gắn với một lớp an toàn

- Lớp an toàn của User KH: Classification. Vd: Clear(S)

- Lớp an toàn của đối tượng KH: Clearance. Vd: Class(O)

KIỂM SOÁT MAC TRONG ORACLE

- Mỗi lớp an toàn được xác định bởi một nhãn - label

- Lớp an toàn = (Mức nhạy cảm, Vùng ứng dụng)

- Label = (Level, Compartment, Group)

+ Level (thành phần bắt buộc): là thành phần không phân cấp, thể hiện mức nhạy cảm

+ Compartment (tuỳ chọn): là các thành phần không phân cấp, sử dụng để phân loại dữ liệu

+ Group (tuỳ chọn): là thành phần phân cấp, được dùng để hỗ trợ phân loại người dùng

MÔ HÌNH BELL - LAPADULA (BLP)

TỔNG QUAN VỀ MÔ HÌNH BLP

- Xuất hiện năm 1975, do quân đội Mỹ

- Phù hợp sử dụng trong các hệ thống của quân đội và chính phủ

- Mục đích: đảm bảo tính bí mật

- Đây là mô hình chính tắc đầu tiên về điều khiển luồng thông tin

- Là một mô hình tĩnh: mức an toàn (nhãn an toàn) không thay đổi

CÁC THUỘC TÍNH CỦA BLP

- Thuộc tính an toàn đơn giản (Not Read Up):

+ Một chủ thể S được phép truy nhập đọc đến một đối tượng O chỉ khi Clear(S) ≥ Class(O)

- Thuộc tính \* (Not Write Down):

+ Một chủ thể S được phép truy nhập ghi lên một đối tượng O chỉ khi Clear(S) ≤ Class(O)

NHẬN XÉT BLP

- Ưu điểm

+ Các nhãn an toàn của các chủ thể và các đối tượng không bao giờ được thay đổi trong suốt thời gian hệ thống hoạt động

- Hạn chế

+ Mới chỉ quan tâm tới tính bí mật

+ Chưa chỉ ra cách thay đổi các quyền truy nhập cũng như cách tạo và xoá các chủ thể cũng như các đối tượng

MÔ HÌNH CSDL ĐA MỨC (MULTILAVEL SECURITY - MLS)

- Hệ thông Multi-level Security (MLS) là hệ thống an toàn nhiều mức, mỗi chủ thể và đối tượng trong đó đều được gắn nhãn an toàn thể hiện mức độ nhạy cảm của các chủ thể và các đối tượng đó

- Mục đích: đảm bảo tính bí mật

- Thường được áp dụng cho lính vực quân sự

- CSDL đa mức: là CSDL mà người dùng và dữ liệu được phân thành các mức ân toàn khác nhau (chẳng hạn như không phân lớp - U, mật - C, tuyệt mật - S, tối mật, - TS)

- Chủ thể khi truy nhập bị giới hạn bởi những điều khiển truy nhập bắt buộc là “not read upm not write down”, theo mô hình của Bell - Lapadula

- Đa thể hiện (polyinstantiation)

+ Là một kỹ thuật trong CSDL cho phép CSDL có thể chứa nhiều thể hiện của cùng một dữ liệu với các mức nhạy cảm khác nhau

+ Trong các DBMS quan hệ, có thể có nhiều bản ghi khác nhau những có cùng một khoá chính với các mức nhạy cảm khác nhau

+ Các bản ghi đa thể hiện là các bản ghi với cùng khoá chính nhưng có các lớp user truy nhập khác nhau gắn với các khoá chính đó

MÔ HÌNH, CHÍNH SÁCH MAC

- Ưu điểm

+ Độ an toàn cao vì sử dụng các nhãn an toàn, phù hợp với các môi trường đòi hỏi độ an toàn nghiêm ngặt như quân sự, quốc phòng

+ Khắc phục được hạn chế của DAC trong vấn đề trao quyền

- Nhược điểm:

+ Phức tạp: việc gắn nhãn không tốt có thể dẫn đến việc gắn nhãn ko đầy đủ hoặc không nhất quán

+ Thiếu kỹ thuật gắn nhãn an toàn tự động: tốn công sức

+ Kênh ngầm: không giải quyết được hoàn toàn tấn công Troạn Horse