GIỚI THIỆU VỀ AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT

Mục đích

- Sinh viên có kiến thức tổng quát về việc bảo mật thông tin.
- Sử dụng một cách hiệu quả các cơ chế bảo mật.

Dữ liệu & Thông tin

- DỮ LIỆU thể hiện thông tin. THÔNG TIN là những điều được diễn giải, rút trích ra được từ DỮ LIỆU.
  - Thông tin là ngữ nghĩa của dữ liệu. Dữ liệu được dùng để chuyển tải và lưu trữ thông tin. Quá trình thao tác trên dữ liệu dẫn xuất ra nhiều thông tin mới.
- Khó phân biệt rạch ròi giữa DỮ LIỆU & THÔNG TIN nhưng đây cũng là nguồn gốc của những khó khăn trong trong lĩnh vực bảo mật máy tính (Computer Security – CS).
- CS nói về quá trình điều khiển truy cập đến thông tin và tài nguyên.
- Điều khiển truy cập đến thông tin là khó, người ta không làm điều này, thay vào đó là việc điều khiển truy cập trên dữ liệu, NHƯNG CHƯA ĐỦ.

Nội dung

1. Lý do phải bảo vệ thông tin
2. Các yêu cầu
3. Các khái niệm cơ bản
4. Yêu cầu và giải pháp

1. Lý do phải bảo vệ thông tin

Tầm quan trọng

- Thông tin mang tầm chiến lược và là tài sản vô giá.
- Sự mất mát, hư hại hoặc sử dụng thông tin sai mục đích không chỉ làm ảnh hưởng đến người sử dụng hay toàn ứng dụng mà còn gây hậu quả không lường cho toàn bộ tổ chức.
- Internet & khả năng của mạng truyền thông làm cho việc truy cập thông tin dễ dàng hơn.

Lý do phải bảo vệ thông tin

- Có nhiều mối đe doạ đến tính an toàn của thông tin:
  - Môi trường đa người dùng (multiuser), mục đích truy cập thông tin là khác nhau.
    - User chỉ được truy cập thông tin cần thiết. Nếu không sẽ có sự truy cập thông tin bất hợp pháp.
  - Dữ liệu có thể bị đánh cắp.
    - Trên đường truyền, đánh cắp thiết bị.
  - Mục đích phá hoại.
    - Virus, DoS (Denial of Service).
  - Yếu tố khách quan.
    - Thiên tai, cháy, mất nguồn, hư hỏng,…
  - …

Ví dụ

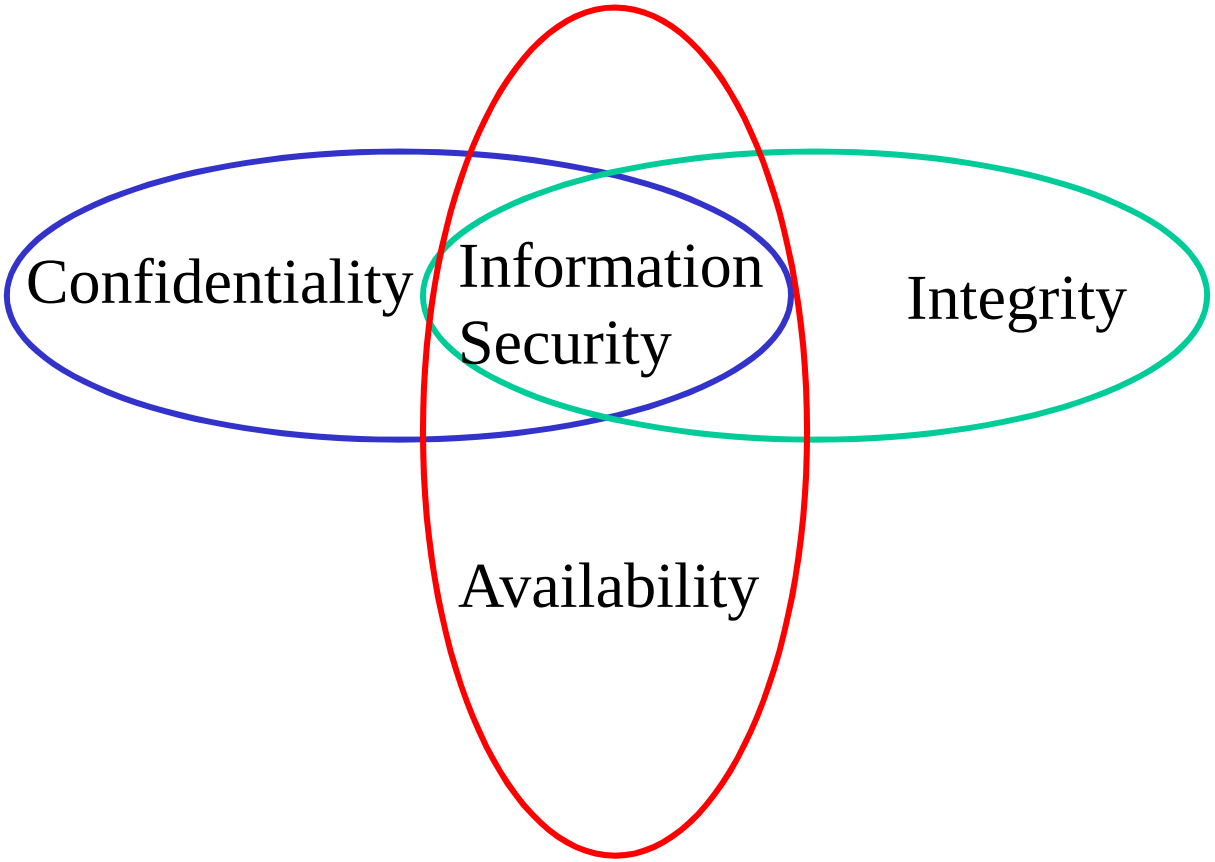
- Cơ sở dữ liệu Moodle:
  - Giáo vụ mới có quyền thêm/ xóa/ sửa trên dữ liệu về môn học mới mở. Sinh viên chỉ có thể xem thông tin này.
  - Giáo viên có thể nhập/ cập nhật điểm cho sinh viên. Sinh viên chỉ có thể xem điểm.

2. Các yêu cầu

Bảo mật thông tin – Các yêu cầu

- *Tính bí mật (Confidentiality)* – người sở hữu dữ liệu không muốn dữ liệu bị đọc bất hợp pháp.
  - Khi dữ liệu liên quan đến 1 cá nhân thì gọi là tính riêng tư (privacy).
- *Tính toàn vẹn (Integrity)* – dữ liệu phải không được sửa đổi bất hợp pháp.
  - Chỉnh sửa dữ liệu bất hợp pháp (unauthorized modifications).
  - Tính xác thực (authenticity), hay dữ liệu là nguyên thủy.
  - Thao tác chỉnh sửa sau (incorrect modifications), gọi là toàn vẹn ngữ nghĩa (semantic integrity).
- *Tính sẵn sàng (Availability)* – đảm bảo những người có quyền sẽ truy cập dữ liệu thành công.

Bảo mật thông tin – Các yêu cầu



Mục đích bảo mật

- Ngăn ngừa (Prevention)
  - Ngăn ngừa những tấn công làm vi phạm chính sách bảo mật.
- Dò tìm (Detection)
  - Dò tìm và có biện pháp ngăn chặn những tấn công làm vi phạm chính sách bảo mật
- Phục hồi (Recovery)
  - Chặn tấn công, đánh giá và sửa chữa thiệt hại.
  - Hệ thống tiếp tục hoạt động một cách đúng đắn ngay cả khi có tấn công.

Bảo mật thông tin - Ở nhiều cấp độ

- Hệ điều hành.
- Mạng.
- Hệ thống quản lý dữ liệu.

3. Các khái niệm cơ bản

Định danh & Xác thực

- Định danh (Identification)
  - Trước khi có thể truy cập vào CSDL, người dùng phải giúp hệ thống nhận diện họ là ai.
- Xác thực (Authentication)
  - Là việc xác minh định danh của người dùng vào thời điểm đăng nhập vào hệ thống.
  - Phương pháp xác thực phổ biến là mật mã (password), ngoài ra có thể dùng máy đọc thẻ, kỹ thuật sinh trắc học (biometric recognition), thiết bị phân tích chữ ký, …

Sự cấp quyền & Điều khiển truy cập

- User authorization
  - Cấp quyền cho từng chủ thể truy cập đến các đối tượng.
    - Chủ thể (subjects): user, program.
    - Đối tượng (objects): database, table, view, procedure, trigger.
- Điều khiển truy cập (access control)
  - Là thủ tục dùng để điều khiển việc cấp quyền.
  - Dựa trên nhiều chính sách khác nhau.

Chính sách và Cơ chế

- Chính sách (Policy) cho biết điều gì được phép thực hiện, điều gì không được phép.
  - Chính sách định nghĩa vấn đề bảo mật cho thông tin.
    - Nguyên lý quyền tối thiểu hay tối đa.
      - Chủ thể chỉ có những quyền tối thiểu cần thiết cho hoạt động của họ hoặc có toàn quyền.
    - Nguyên lý về hệ thống mở hay đóng.
      - HT mở: mặc định là cho phép thực hiện truy cập. Nếu không, hãy dùng câu lệnh không cho truy cập một cách tường minh.
      - HT đóng: mặc định là không cho truy cập. Nếu cho phép thì sẽ dùng câu lệnh cấp quyền một cách tường minh.
      - Trong HT có yêu cầu về an toàn dữ liệu hãy dùng nguyên lý về hệ thống đóng.

Chính sách & Cơ chế (tt)

- Nguyên lý quản trị tập trung hay không tập trung.
  - Ai sẽ bảo trì và quản lý quyền truy cập.
  - Tập trung: 1 người/ nhóm có toàn quyền.
  - Không tập trung: nhiều người điểu khiển quyền truy cập trên các phần khác nhau của CSDL.
  - Ngoài ra, còn có:
    - » Ủy quyền: người có toàn quyền sẽ ủy quyền quản trị lại cho một số người khác.
    - » Quyền thuộc người sở hữu: người có toàn quyền sẽ giao quyền quản trị cho người sở hữu đối tượng dữ liệu.
    - » Quyền cộng tác: quyền cấp cho nhóm, 1 thành viên của nhóm phải được các thành viên còn lại cho phép thì mới được truy cập.
- Nguyên lý về đơn vị dữ liệu: phụ thuộc vào tên, lịch sử, thời gian.
- Nguyên lý về quyền truy cập (access privilege/ access mode): read, write, delete, execute, create.

Chính sách và Cơ chế

- Cơ chế (Mechanism) ép thỏa chính sách.
- Có 3 cơ chế điều khiển truy cập
  - Discretionary access control.
  - Mandatory access control.
  - Role-based access control.
- Các chính sách có thể xung đột nhau, sự không nhất quán có thể tạo ra nhiều điểm yếu.

Các cơ chế điều khiển truy cập

- Điều khiển truy cập nhiệm ý (Discretionary Access Control - DAC)
  - Người sở hữu đối tượng định ra quyền truy cập.
  - Các chủ thể được phép cấp quyền truy cập cho chủ thể khác.
- Điều khiển truy cập bắt buộc (Mandatory Access Control - MAC)
  - MAC giới hạn truy cập của chủ thể đến đối tượng dựa vào mức bảo mật của chủ thể và đối tượng.
  - Việc điều khiển truy cập dựa vào nguyên tắc định trước.
- Điều khiển truy cập dựa trên vai trò (Role Based Access Control - RBAC)

Một số cơ chế bảo mật

- *Xác thực thông tin (Information authentication)*
  - Đảm bảo thông tin là xác thực – dùng cơ chế chữ ký (signature mechanisms)
- *Mã hóa (Encryption)*
  - Bảo vệ thông tin khi được truyền đi qua mạng và khi được lưu.
- *Dò tìm sự mạo danh và những tấn công (intrusion detection)*

Covert channel & Inference

- Bảo vệ thông tin gồm:
  - Bảo vệ dữ liệu trực tiếp thể hiện thông tin
  - Bảo vệ thông tin thông qua
    - Covert channel &
    - Inference

Covert channel & Inference

- Covert channel
  - Một covert channel cho phép truyền đi thông tin gây vi phạm chính sách bảo mật.
- Sự suy diễn (Inference)
  - Sự rút ra thông tin nhạy cảm từ thông tin không nhạy cảm.

Sự suy diễn

SINHVIEN

Tên	GT	NGÀNH	ĐTB
An	Nữ	CNTT	6.3
Hòa	Nam	HTTT	5.8
Nguyệt	Nữ	HTTT	7.0
Nam	Nam	MẠNG	7.5
Tân	Nam	MẠNG	6.6
Nhã	Nữ	CNTT	8.1
Trang	Nữ	CNTT	6.8
Bình	Nam	HTTT	5.0
Tín	Nam	MẠNG	7.0

Sự suy diễn

- Giả sử có chính sách: điểm trung bình của sinh viên là bí mật.
- Tuy nhiên, nếu A là 1 kẻ tấn công biết rằng Nguyệt là sinh viên nữ duy nhất của ngành HTTT. A thực hiện những truy vấn hợp lệ sau:
  - Q1: SELECT Count (*) FROM SINHVIEN WHERE PHAI =‘Nữ’ AND NGÀNH = ‘HTTT’
  - Q2: SELECT Avg (ĐTB) FROM SINHVIEN WHERE PHAI =‘Nữ’ AND NGÀNH = ‘HTTT’

  A biết ĐTB của Nguyệt.

Điều khiển dòng thông tin

- Điều khiển dòng thông tin (Information flow control)
  - Có thể chỉ định tường minh các đối tượng mà 1 chủ thể có thể truy cập, nhưng dòng thông tin chứa đựng trong các đối tượng cần phải được quản lý chặt chẽ.
  - Liên quan đến tính bí mật (chủ thể nào có thể thấy được đối tượng nào) và dòng (điều khiển vấn đề về những gì mà một chủ thể thật sự có thể nhìn thấy).
  - Điều khiển dòng thông tin là kiểm soát được sự suy diễn thông tin dựa trên dữ liệu được phép truy cập.

4. Vấn đề và giải pháp

Giải pháp – tổng quan

- Tính bí mật được ép thỏa bằng cơ chế điều khiển truy cập và mã hóa.
- Tính toàn vẹn đạt được dùng cơ chế điều khiển truy cập và các ràng buộc toàn vẹn về ngữ nghĩa.
- Tính sẵn sàng được đảm bảo dùng cơ chế phục hồi (recovery mechanism) và dùng kỹ thuật dò tìm tấn công từ chối dịch vụ (DoS)

Giải pháp – tổng quan

- Trước tiên, hãy định ra chính sách bảo mật.
- Sau đó, chọn cơ chế để ép thỏa chính sách.
- Cuối cùng, hãy đảm bảo rằng cả cơ chế lẫn chính sách đề ra là vững chắc.

HẾT.