HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA ATTT

BÀI GIẢNG PTTK AN TOÀN MẠNG

PHẦN 2 THIẾT KẾ AN TOÀN MẠNG MÁY TÍNH

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

1. Nguyên lý tối thiểu quyền ưu tiên (Least Privilege)

Nguyên lý tối thiểu quyền ưu tiên phát biểu rằng: *Chủ thể sử dụng (người sử dụng hoặc chương trình máy tính) chỉ nên được trao những quyền ưu tiên mà họ thật sự cần thiết để hoàn thành tác vụ của mình*.

- Phân quyền truy cập

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

2. Nguyên lý ngầm định đảm bảo hoạt động (fail-safe defaults)

- Nguyên lý ngầm định bảo đảm hoạt động phát biểu rằng: *Trừ khi chủ thể sử dụng được trao quyền truy cập đến đối tượng còn không thì nó bị từ chối truy cập (ngầm định) đến đối tượng đó*.
  - Tường lửa
  - Thư mục trong Linux
  - Quyền kế thừa

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

3. Nguyên lý thiết kế tiết kiệm và đơn giản (economy of mechanism):

- Nguyên lý thiết kế tiết kiệm và đơn giản phát biểu rằng: *Các cơ chế an toàn nên càng được thiết kế đơn giản càng tốt*.
  - Sử dụng lại thiết bị
  - Cơ chế AT đơn giản, hiệu quả

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

4. Nguyên lý kiểm soát đầy đủ (complete mediation):

- Nguyên lý kiểm soát đầy đủ yêu cầu sao cho *tất cả các truy cập đến các đối tượng đều được kiểm tra để đảm bảo rằng chúng là được cho phép*.
  - Truy cập dữ liệu chia sẻ
  - Truy cập máy tính
  - Truy cập dịch vụ

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

5. Nguyên lý thiết kế mở (open design):

- Nguyên lý thiết kế mở phát biểu rằng: *An toàn của một cơ chế không nên phụ thuộc vào bí mật của thiết kế hay cài đặt của nó.*
  - Thiết kế thuật toán mật mã
  - Linux
  - Phần mềm mã nguồn mở

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

6. Nguyên lý tách nhỏ quyền ưu tiên (separation of privilege):

- Nguyên lý tách nhỏ quyền ưu tiên phát biểu rằng: *Một hệ thống không nên trao quyền chỉ dựa trên một điều kiện đơn lẻ*.
  - Quyền quản trị
  - Xác thực đa nhân tố

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

7. Nguyên lý cơ chế tối thiểu chia sẻ (least common mechanism):

- Nguyên lý cơ chế tối thiểu chia sẻ phát biểu rằng: Các cơ chế được sử dụng để truy cập đến các tài nguyên không nên cho chia sẻ.
  - Mật khẩu
  - Cơ chế an toàn
  - Mô hình mạng

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

8. Nguyên lý thuận tiện truy cập (psychological acceptability):

- Nguyên lý thuận tiện truy cập phát biểu rằng: Các cơ chế an toàn không nên làm cho tài nguyên khó truy cập hơn so với trường hợp mà các cơ chế an toàn không có mặt.
  - Đăng nhập một lần SSO

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

9. Nguyên lý phân tầng bảo vệ (defense in depth):

- Nguyên lý phân tầng bảo vệ cho rằng không nên chỉ dựa vào một tầng bảo vệ bất kỳ để đạt được an toàn. đa cơ chế an toàn có thể giúp cho đạt được an toàn cao hơn là chỉ có đơn cơ chế an toàn.
  - Bảo vệ lớp vật lý
  - Bảo vệ lớp mạng
  - Bảo vệ lớp phần mềm
  - Bảo vệ lớp chính sách

CHƯƠNG 4.2 NGUYÊN LÝ THIẾT KẾ AN TOÀN

10. Nguyên lý kiểm tra mọi giả thiết an toàn (question assumptions):

- Nguyên lý kiểm tra hay thẩm tra mọi giả thiết an toàn thường kiểm tra lại tất cả các giả thiết về các tác nhân đe dọa, tài sản máy tính và đặc biệt là môi trường của hệ thống.
- VD:
  - Phân quyền
  - Thiết lập luật tường lửa