

**Khoa Khoa Học & Kỹ Thuật Máy Tính - Trường Đại Học Bách Khoa Tp.HCM**

CÂU HỎI VÀ BÀI TẬP CHƯƠNG I

# Môn: MẬT MÃ VÀ AN NINH MẠNG

-o0o-

# Câu hỏi

* 1. Cho biết các nguyên tắc cốt lõi của an toàn thông tin
* Bí mật(Confidentiality): Chỉ bên gửi và bên nhận mới hiểu được nội dung thông điệp.
* Toàn vẹn(Integrity): Đảm bảo thông tin hệ thống, dữ liệu truyền nhận trên mạng không bị thay đổi mà không bị phát hiện.
* Sẳn sàng(Availability): Đảm bảo các dịch vụ trên mạng phải có thể truy cập và có sẵn cho người dùng hợp lệ.
  1. Hãy cho biết khác biệt giữa tấn công thụ động và tấn công chủ động
* Tấn công thụ động là các hành động lấy ra nội dung thông điệp hay phân tích lưu lượng.
  + Rất khó để phát hiện.
  + Cần có biện pháp để ngăn chặn.
* Các nơi mà tấn công thụ động xảy ra: Máy chủ, tháp liên lạc, máy tính desktop, máy fax…
* Tấn công chủ động là các hành động thay đổi nội dung dòng dữ liệu hoặc tạo ra dòng dữ liệu sai lệch.
  + Khá khó khăn để ngăn chặn.
  + Mục tiêu cần thiết là phát hiện và phục hồi từ bất kỳ sự gián đoạn hoặc chậm trễ do chúng gây ra.
  1. Liệt kê các loại tấn công thụ động, tấn công chủ động
* Tấn công chủ động:
  + Giả mạo(masquerade): Mạo danh một thực thể có đặc quyền.
  + Phát lại(replay): Bắt thụ động một đơn vị dữ liệu và truyền lặp lại đơn vị dữ liệu này để tạo ra một hiệu ứng trái phép.
  + Thay đổi nội dung thông điệp: Một số phần của thông điệp hợp pháp được thay đổi, hoặc các thông điệp được trì hoãn hoặc sắp xếp lại, để tạo ra một hiệu ứng trái phép.
  + Từ chối dịch vụ: Ngăn chặn hoặc hạn chế việc sử dụng bình thường hoặc quản lý các tài nguyên trong vấn đề truyền thông.
* Tấn công bị động:
  + Lấy ra nội dung thông điệp:
    - Nghe lén(eavesdropping)
    - Nghe trộm ở một vị trí nào đó mà thông điệp đi qua.
    - Mạng không dây dễ dàng bị tấn công dạng này.
  + Phân tích lưu lượng: Quan sát khuôn mẫu của các thông điệp.
  1. Liệt kê và định nghĩa các cơ chế trong kiến trúc an ninh OSI
* Mã hóa
  + Sử dụng các thuật toán để chuyển đổi dữ liệu thành một hình thức nào đó mà không phải dễ dàng hiểu. Việc chuyển đổi và phục hồi dữ liệu phụ thuộc vào một thuật toán với không có khóa hay một hoặc nhiều khóa.
* Chữ ký số
  + Dữ liệu được nối thêm vào hoặc chuyển đổi mã cho phép người nhận chứng minh nguồn gốc và tính toàn vẹn của dữ liệu.
  + Chống giả mạo.
* Kiểm soát truy cập
  + Một loạt các cơ chế kiểm soát các quyền truy cập vào các tài nguyên.
* Toàn vẹn dữ liệu
  + Một loạt các cơ chế được sử dụng để đảm bảo tính toàn vẹn một đơn vị dữ liệu hoặc dòng các đơn vị dữ liệu.
* Trao đổi xác thực
  + Cơ chế nhằm đảm bảo danh tính một thực thể bằng phương tiện trao đổi thông tin.
* Chèn thông tin trong lưu thông mạng
  + Chèn các bit vào những khoảng trống trong một dòng dữ liệu làm thất bại những nỗ lực phân tích lưu lượng.
* Điều khiển định tuyến
  + Cho phép lựa chọn các tuyến đường đặc biệt an toàn cho dữ liệu nhất định và cho phép thay đổi định tuyến, đặc biệt là khi một hành vi vi phạm an ninh bị nghi ngờ.
* Công chứng
  + Sử dụng một bên thứ ba đáng tin cậy để đảm bảo các thuộc tính nhất định của một giao dịch trao đổi dữ liệu.
  1. Liệt kê và định nghĩa các dịch vụ trong kiến trúc an ninh OSI
* Dịch vụ xác thực: Nhằm xác thực các thực thể hoặc nguồn gốc dữ liệu.
  + Xác thực thực thể ngang hàng nhằm chống các tấn công giả mạo và phát lại.
  + Xác thực nguồn gốc dữ liệu nhằm chống tấn công giả mạo.
* Dịch vụ kiểm soát truy cập: Trong ngữ cảnh an ninh mạng, kiểm soát truy cập là khả năng kiểm soát truy cập đến các hệ thống và các ứng dụng thông qua các liên kết thông tin liên lạc. Để đạt được điều này, mỗi thực thể phải được xác định hoặc chứng thực, sau đó quyền truy cập được thay đổi đối với mỗi thực thể.
* Dịch vụ bí mật dữ liệu, dòng thông tin: Bảo vệ dữ liệu, dòng thông tin được truyền

nhằm chống lại các tấn công thụ động.

* + Dịch vụ bí mật dữ liệu nhằm chống lại tấn công lấy ra nội dung của thông điệp.
  + Dịch vụ bí mật dòng thông tin trên mạng nhằm chống lại tấn công phân tích lưu thông mạng.
  + Áp dụng trên dòng các thông điệp, thông điệp đơn hoặc một vài trường trong thông điệp.
* Dịch vụ toàn vẹn dữ liệu: Đảm bảo dữ liệu nhận được là chính xác và được gởi từ một thực thể có quyền.
  + Dịch vụ toàn vẹn có hướng kết nối: xem xét trên dòng các thông điệp để chắn chắn các thông điệp này là được nhân như khi gởi, không nhân bản, không thêm bớt, không thay đổi, không sắp xếp lại, không phát lại.
  + Dịch vụ toàn vẹn không hướng kết nối: xem xét trên từng thông điệp cụ thể để chắn chắn thông điệp này là được nhân như khi gởi, không thay đổi.
  + Các dịch vụ có khả năng phục hồi hoặc không.
* Dịch vụ chống thoái thác: Chống lại sự từ chối của một trong các thực thể tham gia vào truyền thông hoặc một phần của truyền thông.
  + Dịch vụ chống thoái thác về nguồn gốc: chứng minh rằng thông điệp đã được gởi từ một thực thể cụ thể.
  + Dịch vụ chống thoái thác về đích đến: chứng minh thông điệp đã được nhận từ một thực thể cụ thể

# Câu hỏi trắc nghiệm

## Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin?

* + 1. **Bí mật**
    2. Toàn vẹn
    3. Sẳn sàng
    4. Xác thực

## Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI ?

* + 1. Tấn công từ xa (Remote Attack)
    2. **Tấn công chủ động (Active Attack)**
    3. Tấn công thụ động (Passive Attack)
    4. Cả câu (a) và câu (b) đều đúng

## Cơ chế nào sau đây không cần thiết sử dụng để chống lại tấn công từ chối dịch vụ?

* + 1. **Mã hóa dữ liệu (encipherment)**
    2. Quản lý định tuyến (routing control)
    3. Trao đổi xác thực (authentication exchange)
    4. Quản lý truy cập (access control)

## Cơ chế nào không sử dụng cho dịch vụ xác thực?

* + 1. Mã hóa dữ liệu (encipherment)
    2. Chữ ký số (digital signature)
    3. Trao đổi xác thực (authentication exchange)
    4. **Quản lý truy cập (access control)**

## Cho biết Code Red thuộc vào loại mã độc nào sau đây:

* + 1. Virus
    2. Trojan
    3. Worm
    4. **Là một loại mã độc lai ghép**

# Bài tập

* 1. Hãy xây dựng bảng tương tự như bảng 4.1([1]) mô tả mối quan hệ giữa các dịch vụ và các tấn công trong kiến trúc an ninh OSI
  2. Hãy xây dựng bảng tương tự như bảng 4.1([1]) mô tả mối quan hệ giữa các cơ chế và các tấn công trong kiến trúc an ninh OSI

Trang 1/1