|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **BỘ CÔNG THƯƠNG**  **TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**  **---------------**    **BÁO CÁO MÔN HỌC**  **AN NINH MẠNG NÂNG CAO**    **ĐỀ TÀI:**  **TỔNG QUAN VỀ AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG AN TOÀN CHO CÁC THIẾT BỊ MẠNG  VÀ GIA CỐ HỆ THỐNG**     |  |  |  | | --- | --- | --- | | Giảng viên hướng dẫn | TS. Nguyễn Bá Nghiễn | | | Nhóm sinh viên thực hiện | Phạm Ngọc Bích | 2022700113 | |  | Chu Phương Nam | 2022700114 | |  | Nguyễn Tiến Chung | 2022700128 | |  | Nguyễn Đức Trung | 2022700119 |   ***Hà Nội, 2023*** |

**MỤC LỤC**

[DANH MỤC HÌNH ẢNH 1](#_Toc128992113)

[Lời nói đầu 4](#_Toc128992114)

[CHƯƠNG 1: Tổng quan về an toàn hệ thống và an ninh mạng 5](#_Toc128992115)

[1.1. Một số khái niệm về an toàn thông tin 5](#_Toc128992116)

[ Định nghĩa 5](#_Toc128992117)

[ Tính bảo mật ( 5](#_Toc128992118)

[ Tính toàn vẹn (Integrity) 5](#_Toc128992119)

[ Tính khả dụng (Availability): 5](#_Toc128992120)

[1.2. Một số thách thức của an toàn thông tin (The Challenges of Computer Security) 5](#_Toc128992121)

[1.3. Kiến trúc bảo mật OSI (The OSI security architecture) 6](#_Toc128992122)

[ Tấn công bảo mật (Security attack): 7](#_Toc128992123)

[ Cơ chế bảo mật (Security mechanism): 7](#_Toc128992124)

[ Dịch vụ bảo mật (Security service): 7](#_Toc128992125)

[1.4. Tấn công bảo mật (Security attacks) 7](#_Toc128992126)

[1.4.1 Tấn công thụ động 7](#_Toc128992127)

[1.4.2 Tấn công chủ động 9](#_Toc128992128)

[1.5 Dịch vụ bảo mật (Security services) 12](#_Toc128992129)

[1.5.1 Xác thực (Authentication) 13](#_Toc128992130)

[1.5.2 Điều khiển truy cập (Access control): 13](#_Toc128992131)

[1.5.2 Toàn vẹn dữ liệu (Data integrity) 14](#_Toc128992132)

[1.5.3 Nonrepudiation 14](#_Toc128992133)

[1.6 Cơ chế bảo mật (Security mechanisms) 15](#_Toc128992134)

[1.6.1 Cơ chế bảo mật cụ thể (Specific security mechanisms) 15](#_Toc128992135)

[1.6.2 Cơ chế bảo mật phổ biến (Pervasive security mechanisms) 16](#_Toc128992136)

[1.7 Mối quan hệ giữa Dịch vụ bảo mật và Cơ chế bảo mật (Relationship Between Security Services and Mechanisms) 17](#_Toc128992137)

[1.8 Mô hình an ninh mạng (Model for Network Security) 17](#_Toc128992138)

[CHƯƠNG 2: An toàn cho các thiết bị mạng và gia cố hệ thống 18](#_Toc128992139)

[2.1 Mô hình OSI 18](#_Toc128992140)

[2.2. Tầng vật lý (Physical layer) 19](#_Toc128992141)

[2.3. Tầng liên kết dữ liệu (Data link layer) 20](#_Toc128992142)

[2.4. Tầng mạng (Network layer) 21](#_Toc128992143)

[2.5. Tầng vận chuyển (Transport Layer) 23](#_Toc128992144)

[2.5. Tầng ứng dụng (Application Layer) 24](#_Toc128992145)

[2.6. Gia cố hệ thống mạng (network hardening) 24](#_Toc128992146)

[2.6.1 Gia cố hệ thống tường lửa: 25](#_Toc128992147)

[2.6.2 Gia cố Router, Switch 26](#_Toc128992148)

[2.6.3 Gia cố WLAN 26](#_Toc128992149)

[2.7 Gia cố ứng dụng 27](#_Toc128992150)

[TÀI LIỆU THAM KHẢO 27](#_Toc128992151)

# DANH MỤC HÌNH ẢNH

# LỜI NÓI ĐẦU

Các yêu cầu về bảo mật thông tin trong một tổ chức đã được thay đổi một cách lớn trong vài thập kỉ qua. Trước khi sử dụng rộng rãi các thiết bị xử lý dữ liệu, việc bảo mật thông tin được cho là hiểu quả, chính là sử dụng các vật dụng vật lý như các tủ hồ sơ chắc chắn với khóa kết hợp để lưu trữ các tài liệu nhạy cảm.

Với sự xuất hiện của máy tính, nhu cầu về một công cụ tự động bảo vệ các tệp tin cùng các thông tin khác trong máy tính là hiển nhiên. Điều này đặc biệt đúng với các hệ thống chia sẻ thông tin, và đặc biệt hơn nữa với các hệ thống có thể truy cập thông qua Internet. Các công cụ, các thiết bị, các thiết kế nhằm mục đích bảo vệ dữ liệu và phòng chống “hacker” được gọi chung là Bảo mật máy tính - Computer Security.

Thay đổi lơn thứ hai trong ngành an toàn thông tin là sự ra đời của các hệ thống mạng. Để bảo vệ dữ liệu trong khi truyền tải giữa các máy tính với nhau, các biện pháp bảo mật mạng - network security là cần thiết. Thuật ngữ bảo mật mạng không thật sự chính xác, vì rất nhiều công ty, chính phủ và trường học đều nối các thiết bị xử lý dữ liệu của họ với nhau trên một mạng. Một mạng này thường được gọi là một internet, chính vì vậy thuật ngữ bảo mật internet - Internet Security được sử dụng.

# CHƯƠNG 1: Tổng quan về an toàn hệ thống và an ninh mạng

## 1.1. Một số khái niệm về an toàn thông tin

* Định nghĩa: Theo Sổ tay bảo mật máy tính NIST (NIST95)  
  Sự bảo vệ cung cấp cho một hệ thống thông tin tự động nhằm mục tiêu duy trì tính toàn vẹn, khả dụng và bảo mật của các tài nguyên trong hệ thống (bao gồm phần cứng, phần mềm, firmware, thông tin/ dữ liệu, …).
* Tính bảo mật (**Confidentiality**)
  + Bảo mật dữ liệu (Data confidentiality): Đảm bảo rằng thông tin riêng tư hoặc bí mật không được cung cấp hoặc tiết lộ cho những người không có quyền truy cập chúng.
  + Sự riêng tư (Privacy): Chỉ rõ các các cá nhân có quyền điều khiển, thu thập, lưu trữ, sử dụng các tài nguyên cũng như thông tin của hệ thống.
* Tính toàn vẹn (Integrity):
  + Toàn vẹn dữ liệu (Data integrity): Đảm bảo rằng thông tin và chương trình chỉ được thay đổi theo cách được chỉ định và bởi những người được cho phép.
  + Toàn vẹn hệ thống (System integrity): Đảm bảo rằng hệ thống hoạt động bình thường và không thể bị tác động mà chưa được cho phép kể cả vô tình hay cố tình.
* Tính khả dụng (Availability): Đảm bảo hệ thống hoạt động bình thường dối với các đối tượng đã được cấp phép.

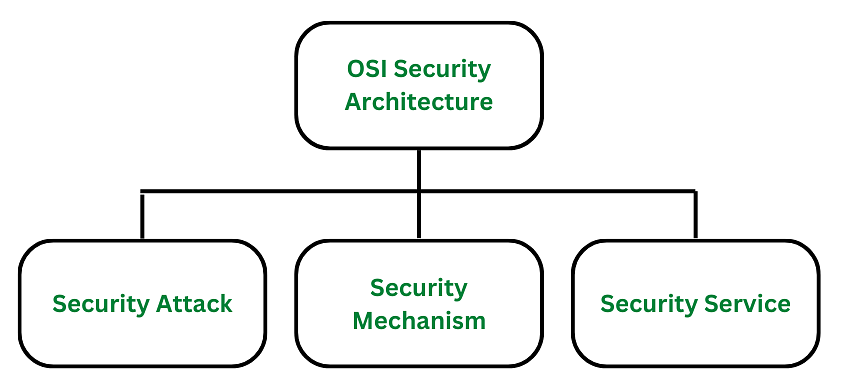
## 1.2. Một số thách thức của an toàn thông tin (The Challenges of Computer Security)

1. Bảo mật không đơn giản với người mới. Các yêu cầu liên quan đến công việc bảo mật thường được đánh nhãn bởi những từ nghe có vẻ khá đơn giản và trực quan như: bảo mật, xác thực, toàn vẹn...Nhưng để hiểu được hoàn các cơ chế hoạt động thì không hề dễ dàng.
2. Trong việc phát triển một cơ chế bảo mật hoặc thuật toán cụ thể, người ta luôn phải xem xét các tấn công có thể đối với những tính năng bảo mật đó. Trong nhiều trường hợp, các tấn công thành công được là nhờ xem xét kỹ lưỡng các cơ chế bằng nhiều cách làm tìm thấy lỗi hổng để rồi khai thác chúng.
3. Các cơ chế bảo mật thường khá phức tạp vì chỉ xử lý đươc một lượng vấn đề nhất định.
4. Có quá nhiều cơ chế cũng như là chuẩn liên quan đến bảo mật. Việc quyết định cái gì sẽ được dùng ở đầu là một việc cần thiết và không hề dễ dàng.
5. Các cơ chế bảo mật thường liên quan đến nhiều thuật toán hoặc giao thức cụ thể.
6. An ninh máy tính và an ninh mạng là cuộc chiến giữa người cố gắng để tìm ra các lỗ hổng của hệ thống với người luôn cố gắng để vá những lỗ hổng này. Kẻ tấn công chỉ cần và quan tâm một lỗ hổng duy nhất trong khi đó những người thiết kế cũng như duy trì hệ thổng cần quan tâm tất cả các điểm yếu để có được một hệ thống hoàn hảo.
7. Người dùng và quản lý hệ thống thường không quan tâm lắm đến bảo mật khi đến khi các lỗi liên quan đến bảo mật xảy ra
8. Bảo mật yêu cầu theo dõi thường xuyên, thậm chí là liên tục, và điều này là một khó khăn lớn trong môi trường quá tải và yêu cầu lớn về tốc độ như hiện nay
9. Người ta vẫn cần xem xét có nên đưa có module liên quan đến bảo mật vào hệ thống thay vì suy nghĩ rằng nó là một phần không thể thiếu của hệ thống.
10. Nhiều người dùng coi bảo mật mạnh gây cản trở hiệu quả cũng như tốc độ của hệ thống.

## 1.3. Kiến trúc bảo mật OSI (The OSI security architecture)

Kiến trúc bảo mật OSI định nghĩa một cách tiếp cận có hệ thống đối với 7 tầng của mô hình OSI nhằm đảm bảo bảo mật trong quá trình truyền dữ liệu trên không gian mạng. Nó đươc phát triển như một tiêu chuẩn quốc tế và đã được cộng đồng đón nhận.

Kiến trúc bảo mật OSI tập trung vào 3 khái niệm:



Hình 1. 1 Mô hình bảo mật OSI

* Tấn công bảo mật (Security attack): Là nỗ lực của một người hoặc một tổ chức nhằm chiếm quyền và truy cập trái phép vào hệ thống nhằm phá vỡ hoặc xâm phạm tính bảo mật của hệ thống, mạng hoặc thiết bị.
* Cơ chế bảo mật (Security mechanism): Một tiến trình (hoặc một thiết bị được tích hợp để thực hiện tiến trình) được thiết kế để phát hiện, ngăn chặn tấn công bảo mật hoặc phục hồi tổn hại sau những cuộc tấn công.
* Dịch vụ bảo mật (Security service): Một tiến trình tăng bảo mật của hệ thống xử lý và truyền phát dữ liệu. Thực hiện đếm các cuộc tấn công, đưa ra quyết định tạo ra hoặc sử dụng cơ chế bảo mật nào cho hệ thống.

## 1.4. Tấn công bảo mật (Security attacks)

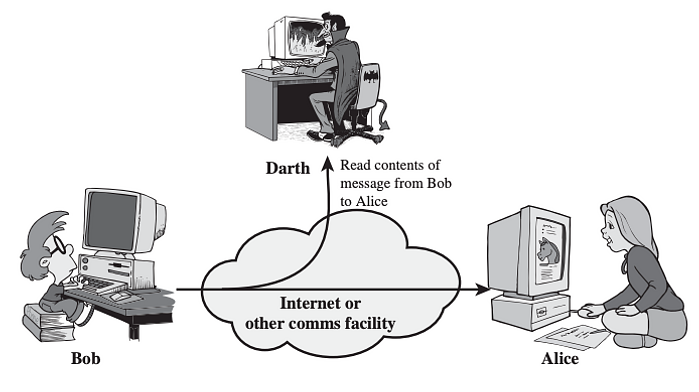
### 1.4.1 Tấn công thụ động

Các cuộc tấn công thụ động bản chất giống như nghe lén, theo dõi khi mà dữ liệu được truyền đi. Tấn công thụ động có 2 kiểu là lấy cắp nội dung tin nhắn (release of message contents) và phân tích lưu lượng (traffic analysis).

Tấn công thụ động khó bị phát hiện vì không thay đổi dữ liệu hoặc tài nguyên hệ thống. Thông thường cả người gửi và người nhận tin nhắn đều không thể xác định được tin nhắn được đọc bởi bên thứ 3. Tuy nhiên mã hóa dữ liệu trước khi gửi đi là một cách hữu hiệu để ngăn chặn các cuộc tấn công thụ động thay vì cố tình tìm kiếm và phát hiện các cuộc tấn công.

#### Lấy cắp nội dung tin nhắn (release of message contents)

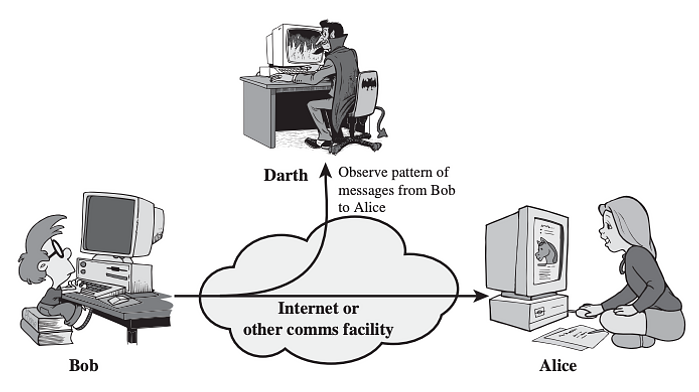
Một cuộc nói chuyện qua điện thoại, một tin nhắn, một tệp tin được gửi đi có thể chứa các thông tin nhạy cảm và bảo mật. Chúng ta cần ngăn những kẻ tấn công biết được, lấy được những thông tin này.



Hình 1. 3 Lấy cắp nội dung tin nhắn

#### Phân tích lưu lượng (traffic analysis)

Giả sử rằng chúng ta có cách che giấu nội dung của tin nhắn hoặc các thông tin khác để đối thủ, ngay cả khi họ bắt được tin nhắn thì cũng không thể trích xuất thông tin từ thông điệp. Kỹ thuật phổ biến để che giấu nội dung là mã hóa. Trong trường họp này kẻ tấn công không thể được được nội dung của tin nhắn mà chỉ hiểu được kiểu mẫu và độ dài của mã hóa. Kẻ tấn công thực hiện phân tích các mẫu và siêu dữ liệu của lưu lượng mạng để thu thập thông tin về hệ thống, mạng hoặc thiết bị.



Hình 1. 4 Phân tích lưu lượng

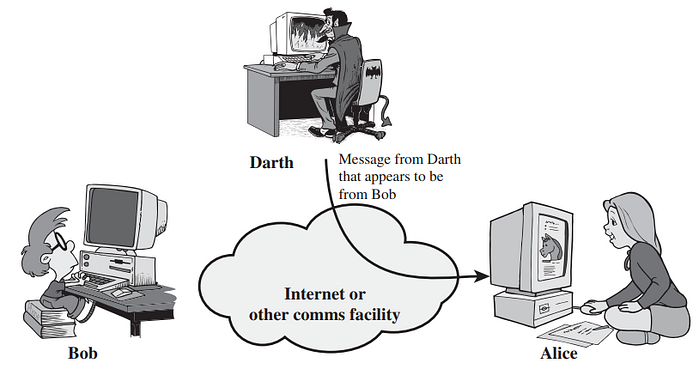
### 1.4.2 Tấn công chủ động

Tấn công chủ động liên quan đến thay dổi luồng dữ liệu (data stream) hoặc tạo ra một luồng dữ liệu sai.

Khó có thể ngăn chặn tuyệt đối các cuộc tấn công chủ động vì có quá nhiều lỗ hổng tiềm ẩn về mặt vật lý, phần mềm và cả mạng. Chính vì thế mục tiêu chính sẽ là phát hiện rồi phục hồi sau bất kỳ sự gián đoạn hoặc chậm trễ nào do các cuộc tấn công gây ra.

#### Giả mạo (Masquerade)

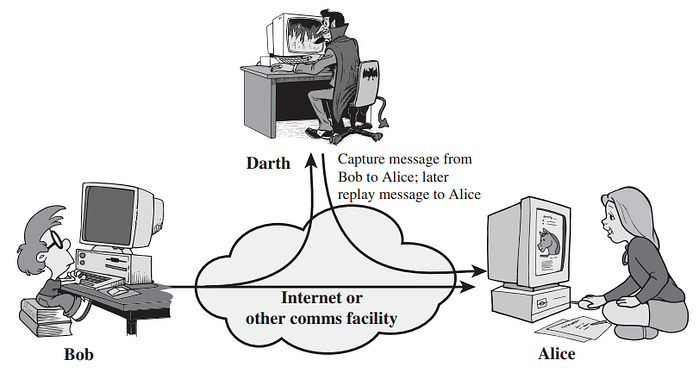
Diễn ra khi kẻ tấn công giả mạo một thực thể đã được xác thực để có được quyền truy cập trái phép vào hệ thống. Tấn công giả mạo thường đi kèm theo hình thức tấn công chủ động khác.



Hình 1. 5 Tấn công chủ động – Giả mạo

#### Phát lại (Replay)

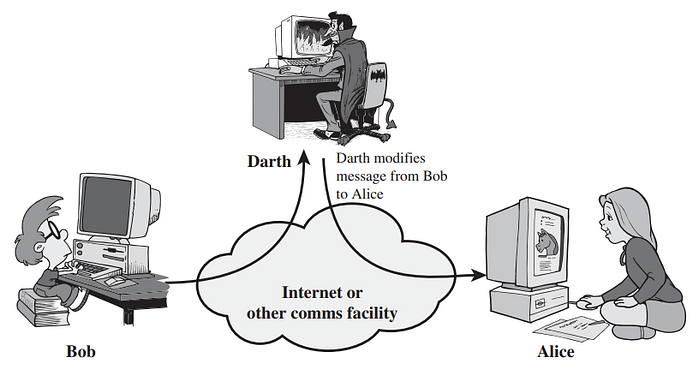
Kẻ tấn công bắt lấy một tin nhắn được truyền đi thông qua một kênh bị động sau đó phát lại một tin nhắn gian lận khác hoặc trì hoãn nó một thời gian.



Hình 1. 6 Tấn công chủ động – Phát lại

#### Sửa đổi tin nhắn (Modification of message)

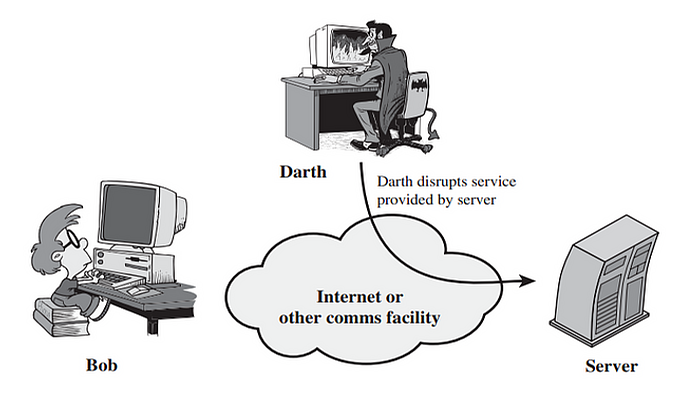
Kẻ tấn công sửa đổi tin nhắn đã được gửi đi khiến cho người nhận có thể nhận được một tin nhắn không an toàn hoặc vô nghĩa. Kiểu tấn công này sử dụng để thao túng nội dung tin nhắn hoặc làm gián đoạn quá trình giao tiếp.



Hình 1. 7 Tấn công chủ động – Sửa đổi tin nhắn

#### Từ chối phục vụ (Denial of service - DoS)

Kẻ tấn công gửi một lượng truy cập lớn vào hệ thống, mạng, hoặc thiết bị, khiến cho thực thể bị tấn công từ chối hoạt động kể cả đối với người dùng đã được xác thực do bị quá tải.



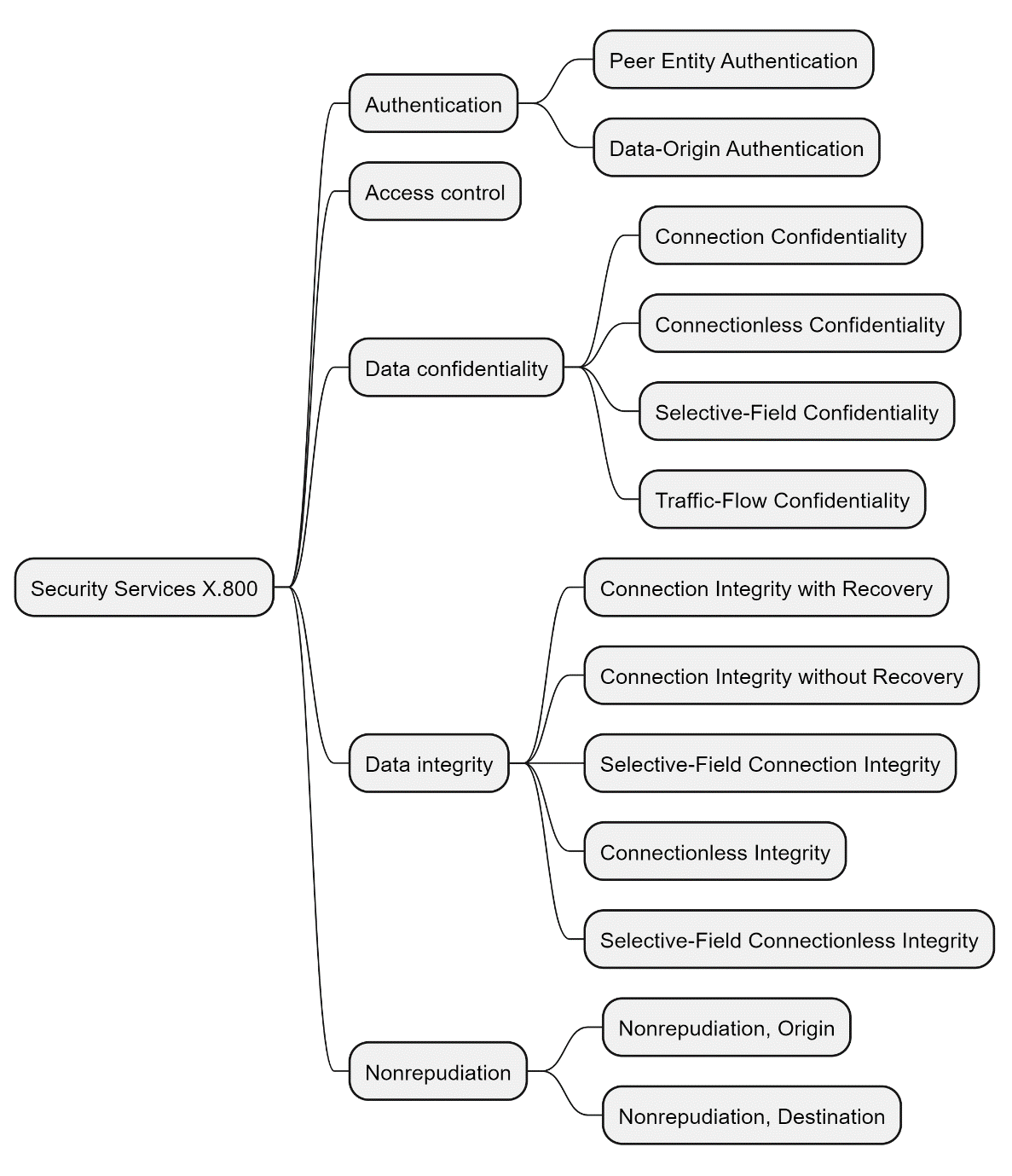
Hình 1. 8 Tấn công chủ động – Từ chối dịch vụ (DoS)

## 1.5 Dịch vụ bảo mật (Security services)

X.800 định nghĩa 1 dịch vụ bảo mật là 1 dịch vụ đảm bảo an toàn của hệ thống và quá trình truyền dữ liệu.

RFC 2828 định nghĩa một tiến trình hoặc một dịch vụ thực hiện bảo vệ đặc biệt cho tài nguyên của hệ thống là các dịch vụ bảo mật, thứ mà thực hiện các chính sách và các cơ chế bảo mật.

X800 chia các dịch vụ này vào 5 loại và có 14 dịch vụ đặc biệt (specific services).



Hình 1. 9 Dịch vụ bảo mật

### Xác thực (Authentication)

Là quá trình xác thực người dùng hoặc thiết bị nhằm mục đích cấp phép hoặc từ chối truy cập vào hệ thống hoặc thiết bị. Khi khởi tạo kết nối cần đảm bảo 2 thực thể phải được xác thực sau đó kết nối của 2 thực thể phải được đảm bảo là không bị cân thiệp.

* Xác thực ngang hàng (Peer entity authentication): Sử dụng cùng với kết nối logic để xác thực các thực thể được kết nối. Hai thực thể được coi là ngang hàng nếu như giao tiếp với nhau cùng một giao thức nhưng khác hệ thống. Xác thực ngang hàng sử dụng khi khởi tạo hoặc trong quá trình truyền dữ liệu trên một kết nối. Bên cạnh đó liên tục xác nhận rằng thực thể cần được xác thực không phải là thực thể giả mạo hoặc được phát lại (replay) của kết nối trước đó.
* Xác thực nguồn gốc dữ liệu (Data-Origin Authentication): Đảm bảo dữ liệu mà người nhận nhận được là giống với thông tin gửi đi trong truyền tải phi kết nối (connectionless transfer). Kiểu dịch vụ này không hỗ trợ chống lại việc nhân bản dữ liệu.

### 1.5.2 Điều khiển truy cập (Access control):

Liên quan đến việc sử dụng các chính sách và thủ tục để xác định ai được phép truy cập các tài nguyên cụ thể trong một hệ thống. Là khả năng giới hạn và điều khiển các truy cập vào máy chủ hệ thống. Để làm được vậy mỗi thực thể muốn truy cập vào hệ thống trước tiên cần phải được xác thực.

* Bảo mật dữ liệu (Data confidentiality): Bảo vệ dữ liệu khỏi bị truy cập hoặc tiết lộ một cách trái phép.
* Bảo mật kết nối (Connection confidentiality): Bảo vệ dữ liệu của tất cả người dùng trên một kết nối.
* Bảo mật phi kết nối (Connectionless confidentiality): Bảo vệ dữ liệu của tất cả người dùng trong một khối dữ liệu đơn (a single data block).
* Bảo mật trường được chọn (Selective-Field Confidentiality): Bảo mật các trường được chọn trong dữ liệu người dùng trên một kết nối hoặc trong một khối dữ liệu.
* Bảo mật lưu lượng luồng dữ liệu (Traffic-Flow confidentiality): Là các kỹ thuật phát minh ra để ẩn/ làm giả các mẫu lưu lượng (traffic pattern) nhằm ngăn các cuộc tấn công bằng cách phân tích lưu lượng (statistical traffic analysis attacks).

### **Toàn vẹn dữ liệu (Data integrity)**

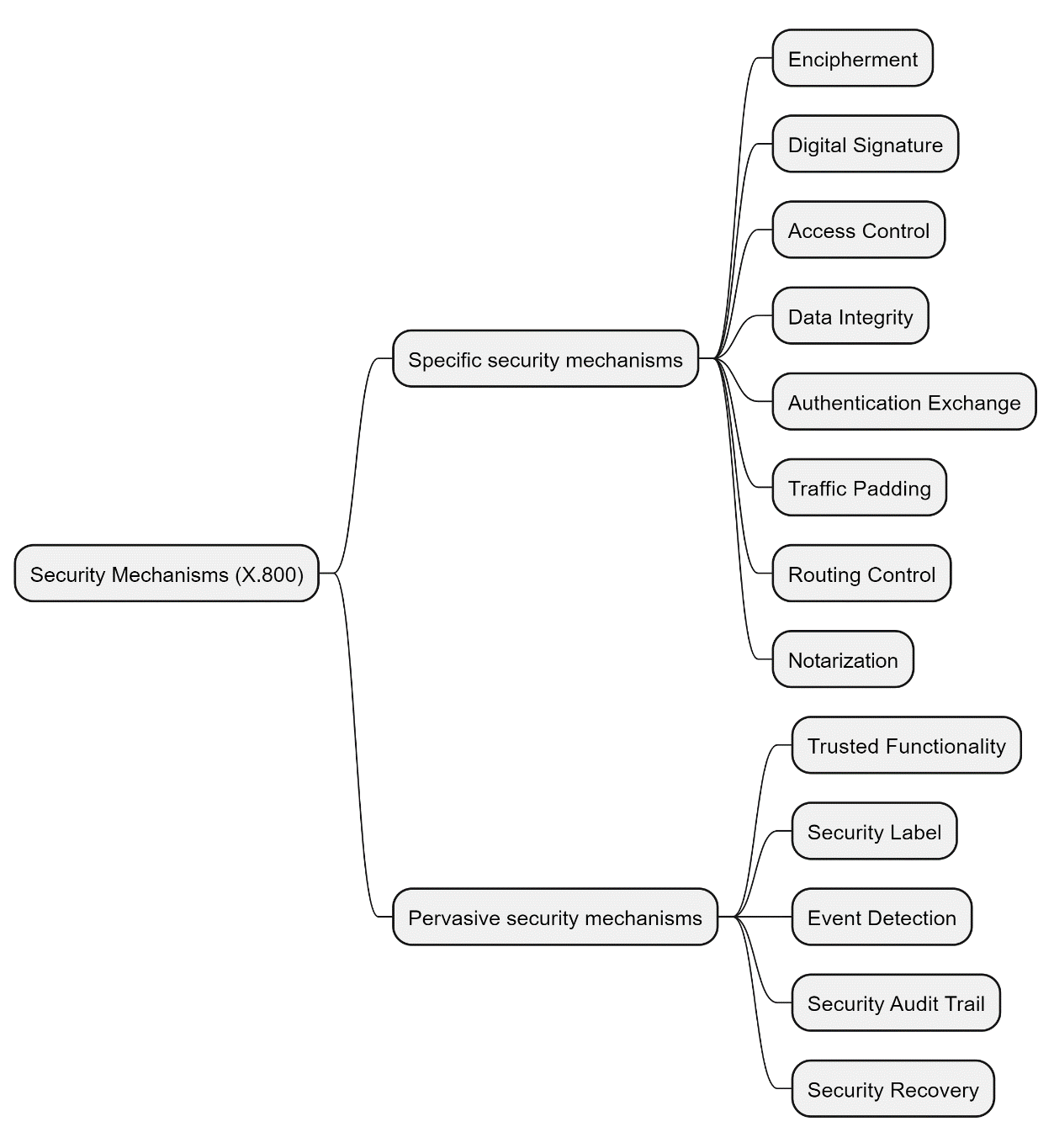
Đảm bảo rằng dữ liệu nhận được chính xác được gửi đi bởi một thực thể đã được cấp phép.

* **Connection integrity with recovery:** Đảm bảo mọi dữ liệu của người dùng đã kết nối chính xác, nhất quán. Phát hiện mọi thao tác chỉnh sửa, thêm, xóa, hoặc phát phát dữ liệu trên đường truyền. Nếu phát hiện các thao tác trên dịch vụ sẽ cố gắng khôi phục dữ liệu về tình trạng "toàn vẹn".
  + **Connection integrity without recovery:** Chỉ ra các hành động có can thiệp tới dữ liệu nhưng không cố gắng khôi phục dữ liệu.
  + **Selective-Field Connection integrity**: Cung cấp tính đúng đắn cho một số trường thuộc khối dữ liệu, chỉ ra các trường đã bị sửa, thêm, xóa, hoặc phát lại trong số các trường đã chọn.
  + **Connectionless integrity:** Cung cấp tính toàn vẹn của một khối dữ liệu phi kết nối (connectionless data block), phát hiện sửa đổi và phát lại dữ liệu.
  + **Selective-Field Connectionless Integrity:** Cung cấp tính đúng đắn cho một số trường thuộc khối dữ liệu phi kết nối (connectionless data block), chỉ ra trường nào bị thay đổi trong các trường đã chọn.

### Nonrepudiation

Ngăn chặn người nhận hoặc người gửi từ chối một tin nhắn đã được truyền đi. Như vậy, khi mà một tin nhắn đã được gửi đi, người nhận có thể chứng minh rằng người gửi đã thực sự gửi tin nhắn đó. Tương tự, khi mà tin nhắn được nhận, người gửi cũng có thể chứng minh rằng người nhận đã thật sự nhận được tin nhắn đó.

## 1.6 Cơ chế bảo mật (Security mechanisms)



Hình 1. 10 Cơ chế bảo mật theo X.800

### 1.6.1 Cơ chế bảo mật cụ thể (Specific security mechanisms)

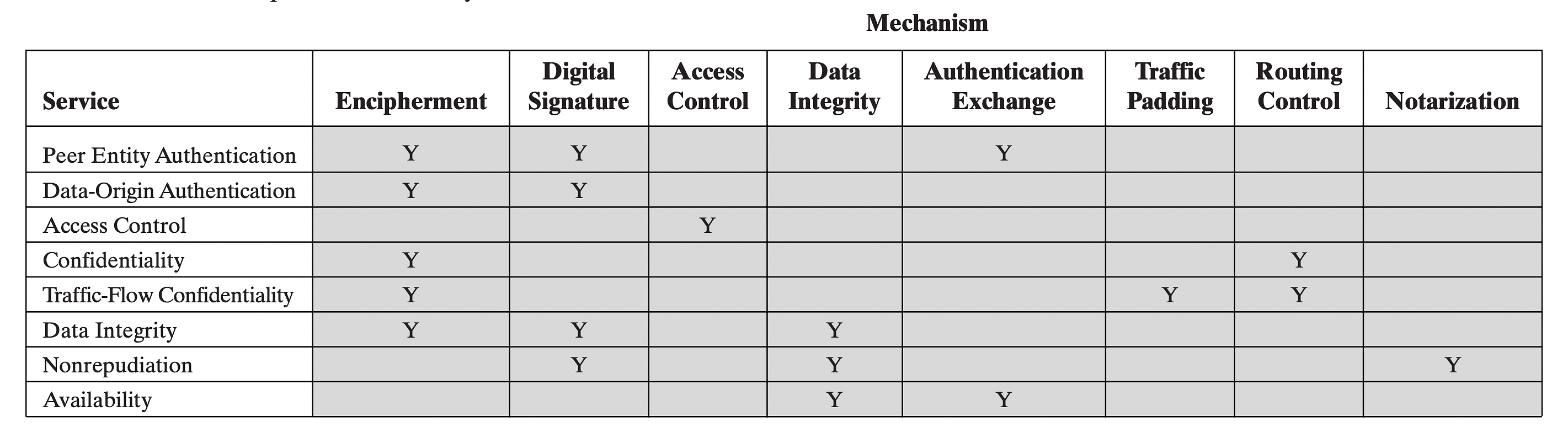
* **Mã hóa (Encipherment):** Sử dụng các thuật toán để biến đổi dữ liệu sang một dạng khó hiểu. Việc mã hóa và giả mã có thể không phụ thuộc 0, 1 hoặc nhiều khóa.
* **Chữ ký số (Digital Signature):** Dữ liệu được thêm vào tin nhắn hoặc tài liệu cho phép người nhận xác thực được nguồn gốc và tính đúng đắn của thông tin nhận được.
* **Kiểm soát truy cập (Access Control):** cơ chế kiểm tra các quyền truy cập vào tài nguyên.
* **Toàn vẹn dữ liệu (Data Integrity):** Các cơ chế sử dụng để đảm bảo tính đúng đắn của khối dữ liệu hoặc luồng dữ liệu (stream of data units).
* **Trao đổi xác thực (Authentication Exchange):** Một cơ chế xác thực danh tính của thực thể bằng cách trao đổi thông tin. Một đối tượng giải mã thành công một tin nhắn bằng cách sử dụng 1 khoá trong cặp khoá (key pair). Họ có thể suy ra người có khóa tương ứng, cũng chính là danh tính người gửi tin nhắn.
* **Đệm lưu lượng (Traffic Padding):** Là kỹ thuật chèn các bit vào các khoảng trống trong luồng dữ liệu (data stream) nhằm hạn chế, gây cản trở việc phân tích lưu lượng.
* **Kiểm soát định tuyến (Routing Control):** Cho phép lựa chọn đường đi về mặt vật lý cho một số dữ liệu, có thể thay đổi đường đi này, đặc biệt là khi có nghi ngờ về việc thiếu bảo mật.
* **Công chứng (Notarization):** Sử dụng một bên thứ 3 để đảm bảo bảo mật trong quá trình truyền dữ liệu.

### 1.6.2 Cơ chế bảo mật phổ biến (Pervasive security mechanisms)

Là các cơ chế không dành riêng cho bất kỳ giao thức hay dịch vụ bảo mật OSI cụ thể nào.

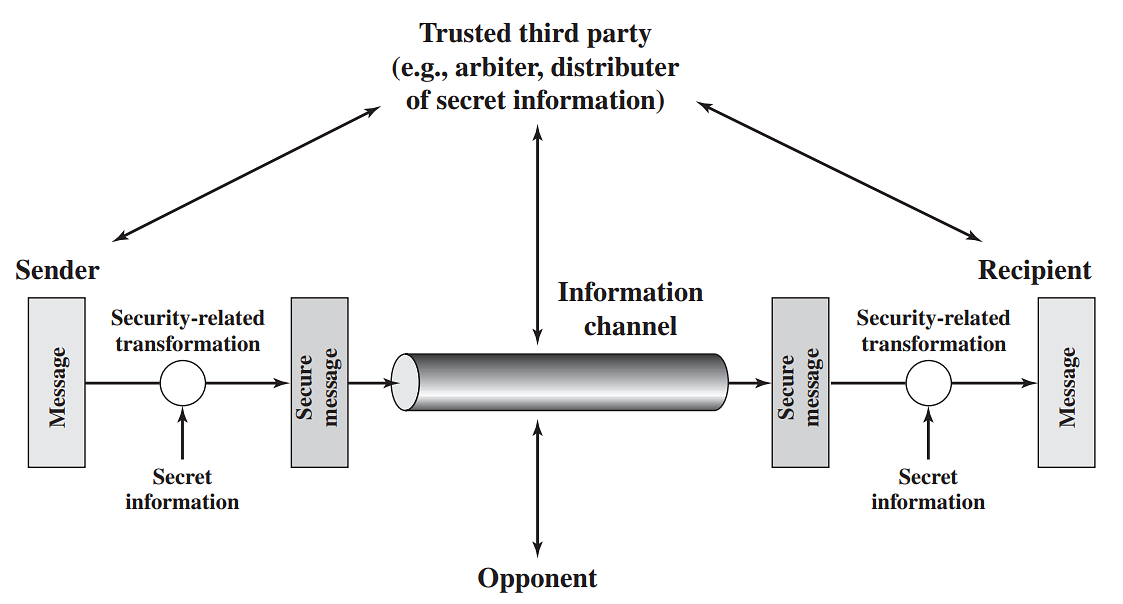
* **Chức năng đáng tin cậy (Trusted Functionality):** thứ được coi là đúng đối với một số tiêu chí.
* **Nhãn bảo mật (Security Label):** Tạo ràng buộc với một tài nguyên (hoặc một khối dữ liệu) để đặt tên hoặc định rõ các thuộc tính bảo mật của tài nguyên đó.
* **Phát hiện sự kiện (Event Detection):** Phát hiện các sự kiện liên quan tới bảo mật.
* **Con đường kiểm tra bảo mật (Security Audit Trail):** Thu tập dữ liệu có tiềm năng để thuận tiện đánh giá bảo mật.
* **Phục hồi bảo mật (Security Recovery):** Tuỳ theo yêu cầu của cơ chế, chẳng hạn như các chức năng quản lý và xử lý sự kiện cần các thao khôi phục dữ liệu.

## 1.7 ****Mối quan hệ giữa Dịch vụ bảo mật và Cơ chế bảo mật (Relationship Between Security Services and Mechanisms)****



Hình 1. 11 Mối quan hệ giữa Dịch vụ bảo mật và Cơ chế bảo mật

## 1.8 Mô hình an ninh mạng (Model for Network Security)



Hình 1. 12 Mô hình an ninh mạng

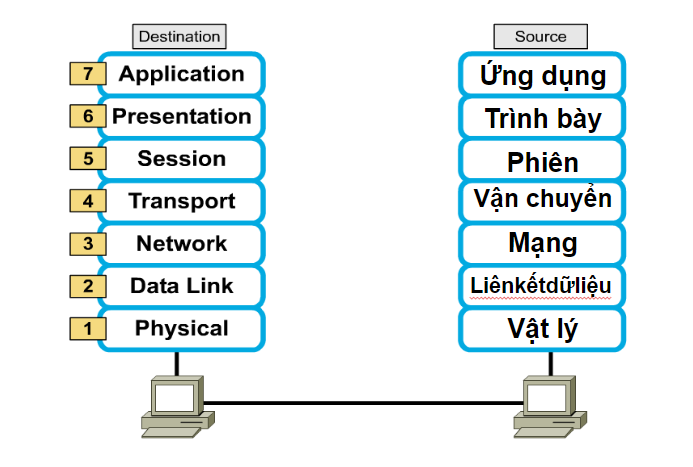
Các yếu tố bảo mật được bật khi cần thiết hoặc theo mong muốn của người sử dụng nhằm bảo vệ thông tin được gửi đi khỏi các kẻ tấn công - người mà gây ra các mối đe dọa liên quan đến bảo mật, xác thực, và nhiều vấn đề khác.

**Tất cả các kỹ thuật cung cấp bảo mật đều có 2 phần:**

* Làm biến đổi thông tin trước khi gửi đi
  + - Mã hóa tin nhắn khiến kẻ tấn công không thể biết được nội dung tin nhắn.
    - Ký số - một số thông tin được thêm vào nội dung gửi đi nhằm xác thực và định danh người gửi.
  + Một thông tin bí mật chỉ được biết bởi hai thực thể tham gia giao tiếp
    - Khóa (key) được biết bởi hai đầu cuộc đối thoại tham gia vào quá trình mã hóa – giải mã, cũng như ký – xác thực.

# CHƯƠNG 2: An toàn cho các thiết bị mạng và gia cố hệ thống

## 2.1 Mô hình OSI



Hình 2. 1 Mô hình mạng OSI

Mô hình OSI được phát triển bởi Tổ chức tiêu chuẩn hóa quốc tế (ISO) và được công bố vào năm 1984.

Mô hình OSI (Open Systems Interconnection) hay còn gọi là Mô hình tham chiếu kết nối các hệ thông mở là một thiết kế dựa vào nguyên lý phân tầng mô tả cách mà thông tin được truyền tải qua mạng. Sinh ra nhằm khắc phục tình trạng không tương thích giữa các mạng trên thị trường gây cản trở việc kết nối giữa các người dùng sử dụng các mạng khác nhau.

Mô hình OSI gồm 7 tầng và mỗi lớp thực hiện một tác vụ cụ thể để truyền tải thông tin.

1. **Tầng vật lý (Physical Layer):** Tầng này xác định các kỹ thuật truyền dẫn dữ liệu qua các thiết bị vật lý như cáp, đường truyền, tín hiệu và bộ chuyển đổi. Nhiệm vụ của tầng này là đảm bảo dữ liệu được truyền qua môi trường truyền dẫn một cách tin cậy.
2. **Tầng liên kết dữ liệu (Data Link Layer):** Tầng này quản lý các giao tiếp trực tiếp giữa các thiết bị trong cùng một mạng. Tầng này cũng có trách nhiệm kiểm soát lỗi và đảm bảo tính toàn vẹn của dữ liệu trên đường truyền.
3. **Tầng mạng (Network Layer):** Tầng này xác định cách thức định tuyến dữ liệu giữa các mạng khác nhau. Tầng này cũng có trách nhiệm định danh các thiết bị trên mạng và đảm bảo việc truyền dữ liệu giữa các thiết bị trên mạng.
4. **Tầng giao vận (Transport Layer):** Tầng này xác định các dịch vụ giao vận như TCP (Transmission Control Protocol) và UDP (User Datagram Protocol) để đảm bảo tính toàn vẹn, độ tin cậy và hiệu suất của dữ liệu trên mạng.
5. **Tầng phiên (Session Layer):** Tầng này đảm bảo tính liên tục của các phiên giao dịch giữa các thiết bị trên mạng. Tầng này cũng xác định cách thức thiết lập, duy trì và đóng các phiên trên mạng.
6. **Tầng trình diễn (Presentation Layer):** Tầng này xử lý định dạng và mã hóa dữ liệu để đảm bảo tính tương thích giữa các thiết bị trên mạng.
7. **Tầng ứng dụng (Application Layer):** Tầng cuối cùng của mô hình OSI cung cấp các phương tiện cho người dùng truy cập và sử dụng các dịch vụ của mô hình OSI.

## 2.2. Tầng vật lý (Physical layer)

Tầng vật lý (Physical layer) là tầng đầu tiên của mô hình OSI. Mô tả các đặc trưng vật lý của mạng. Tầng này định nghĩa các thông số ký thuật cần thiết để truyền dữ liệu qua các phương tiện truyền dẫn như cáp, bộ chuyển đổi, … Các thông số kỹ thuật này bao gồm tốc độ truyền dữ liệu, điều chế tín hiệu, định dạng tín hiệu và kiểm soát lỗi.

Điều chế tín hiệu là quá trình biến đổi tín hiệu từ dạng cơ học, điện tử, ánh sáng hay sóng radio thành một tín hiệu mới phù hợp với yêu cầu truyền tải thông tin trong một hệ thống truyền thông nào đó. Quá trình điều chế tín hiệu được thực hiện bằng cách sử dụng các thiết bị điện tử như modulator và các kỹ thuật xử lý tín hiệu để thay đổi các thông số của tín hiệu ban đầu. Việc điều chế tín hiệu là một bước quan trọng trong việc truyền tải thông tin trong các hệ thống truyền thông như radio, truyền hình, điện thoại, và Internet. Các phương pháp điều chế tín hiệu bao gồm ASK, FSK, PSK và QAM. ASK điều chế tín hiệu bằng cách sử dụng các tín hiệu đơn giản như sóng vuông. FSK sử dụng các tín hiệu có tần số khác nhau. PSK sử dụng các tín hiệu với pha khác nhau. QAM kết hợp cả ASK và PSK để điều chế tín hiệu.

Định dạng tín hiệu là xác định cách thức biểu diễn dữ liệu trên đường truyền. Các định dạng tín hiệu bao gồm các chuỗi bit đơn giản, các chuỗi bit được mã hóa hoặc các chuỗi bit được biểu diễn dưới dạng tín hiệu analog. Các chuỗi bit đơn giản có thể được biểu diễn bằng các mức điện trên đường truyền. Các chuỗi bit được mã hóa có thể được mã hóa dưới dạng mã Manchester hoặc NRZ. Các chuỗi bit được biểu diễn dưới dạng tín hiệu analog bao gồm AM, FM và PM.

## 2.3. Tầng liên kết dữ liệu (Data link layer)

Tầng liên kết dữ liệu (Data Link Layer) là tầng thứ hai trong mô hình OSI. Nó cung cấp các dịch vụ để đảm bảo việc truyền dữ liệu đáng tin cậy giữa các thiết bị trên mạng. Tầng này có nhiệm vụ chuyển dữ liệu từ tầng vật lý thành các khung dữ liệu (frame) có thể được gửi qua mạng.

**Các nhiệm vụ chính của tầng liên kết dữ liệu bao gồm:**

* **Đóng gói dữ liệu:** Dữ liệu được chia thành các khung dữ liệu để truyền đi trên mạng. Mỗi khung dữ liệu bao gồm các thông tin như địa chỉ MAC (Media Access Control), các thông số kiểm soát lỗi và dữ liệu thực sự.
* **Kiểm soát truy cập vào mạng:** Tầng liên kết dữ liệu đảm bảo rằng các thiết bị trên mạng không xung đột khi cùng truy cập vào mạng. Các giao thức kiểm soát truy cập vào mạng được sử dụng ở tầng này bao gồm CSMA/CD (Carrier Sense Multiple Access/Collision Detection) và Token Ring.
* **Kiểm tra lỗi:** Tầng liên kết dữ liệu đảm bảo rằng các khung dữ liệu được gửi qua mạng không bị lỗi. Các kỹ thuật kiểm tra lỗi bao gồm kiểm tra số tiếp theo (CRC - Cyclic Redundancy Check), kiểm tra dư (Parity Check) và kiểm tra lỗi bit (Bit-Error Rate Testing).
* **Điều khiển luồng dữ liệu:** Tầng liên kết dữ liệu đảm bảo rằng dữ liệu được gửi đi ở mức độ phù hợp với khả năng xử lý của thiết bị nhận. Điều này được đảm bảo bằng cách sử dụng các giao thức điều khiển luồng dữ liệu như Stop-and-Wait và Go-Back-N.
* **Định danh thiết bị:** Tầng liên kết dữ liệu xác định và quản lý địa chỉ MAC của các thiết bị trên mạng. Địa chỉ MAC là một địa chỉ vật lý duy nhất được gán cho mỗi thiết bị trên mạng để định danh nó trong quá trình truyền dữ liệu.

**Các thành phần chính của tầng liên kết dữ liệu bao gồm:**

* **MAC (Media Access Control):** Đây là phần của tầng liên kết dữ liệu quản lý việc truy cập vào mạng và phân bổ tài nguyên mạng cho các thiết bị. Mỗi thiết bị trên mạng sẽ có một địa chỉ MAC riêng để định danh nó trong quá trình truyền dữ liệu.
* **LLC (Logical Link Control):** Đây là phần của tầng liên kết dữ liệu xử lý các dịch vụ truyền dữ liệu logic giữa các thiết bị trên mạng. LLC quản lý cơ chế kiểm soát lỗi, điều khiển luồng dữ liệu và quản lý địa chỉ logic của các thiết bị trên mạng.

**Các giao thức của tầng liên kết dữ liệu được chia thành hai loại chính:**

* **Giao thức liên kết dữ liệu điểm – điểm (point-to-point):** Giao thức này được sử dụng để truyền dữ liệu giữa hai thiết bị trực tiếp kết nối với nhau. Ví dụ về giao thức này là HDLC và PPP.
* **Giao thức liên kết dữ liệu đa điểm (multiple access):** Giao thức này được sử dụng để truyền dữ liệu giữa nhiều thiết bị trên cùng một mạng. Các giao thức liên kết dữ liệu multiple access phổ biến bao gồm Ethernet, Token Ring và FDDI (Fiber Distributed Data Interface).

## 2.4. Tầng mạng (Network layer)

Tầng mạng (Network Layer) là tầng thứ ba trong mô hình OSI, nó cung cấp các dịch vụ cho việc truyền dữ liệu từ nguồn tới đích qua một mạng. Nó là tầng trung gian giữa tầng liên kết dữ liệu và tầng vận chuyển. Tầng này đảm bảo việc truyền dữ liệu qua một mạng có thể được thực hiện một cách hiệu quả và đáng tin cậy.

Tầng mạng có vai trò quan trọng trong việc bảo mật mạng. Các kỹ thuật bảo mật như tường lửa (firewall), ảo hóa mạng (virtual private network - VPN), và IDS/IPS (Intrusion Detection/Prevention System) đều sử dụng các chức năng của tầng mạng để kiểm soát và giám sát việc truyền tải dữ liệu trên mạng.

**Các chức năng chính của tầng mạng bao gồm:**

* **Định tuyến (Routing):** Tầng mạng xác định đường đi tốt nhất cho dữ liệu đi từ nguồn đến đích. Định tuyến có thể được thực hiện bằng các giao thức định tuyến, bao gồm cả định tuyến tĩnh và định tuyến động.
* **Chuyển tiếp (Forwarding):** Tầng mạng chuyển tiếp dữ liệu đến địa chỉ đích thông qua một mạng. Chuyển tiếp dữ liệu có thể được thực hiện bằng các bảng định tuyến hoặc các giao thức định tuyến.
* **Phân mảnh (Fragmentation):** Tầng mạng có thể phân mảnh các gói tin dữ liệu thành các phần nhỏ hơn để truyền qua các kênh truyền có băng thông thấp hơn.
* **Kiểm soát tắc nghẽn (Congestion Control):** Tầng mạng đảm bảo rằng không có quá nhiều dữ liệu được gửi qua mạng một lúc, từ đó giảm thiểu sự cạnh tranh tài nguyên mạng và tăng hiệu suất truyền dữ liệu.

**Các giao thức phổ biến của tầng mạng:**

* **IPv4 (Internet Protocol version 4):** Đây là giao thức tầng mạng phổ biến nhất hiện nay. Nó được sử dụng để xác định địa chỉ IP của thiết bị và địa chỉ mạng để chuyển tiếp các gói tin dữ liệu trên mạng.
* **IPv6 (Internet Protocol version 6):** Đây là phiên bản mới của giao thức IPv4, cung cấp nhiều địa chỉ IP hơn để hỗ trợ cho sự phát triển của Internet.
* **OSPF (Open Shortest Path First):** Đây là một giao thức định tuyến động, được sử dụng để xác định đường đi tối ưu giữa các địa chỉ mạng khác nhau.
* **BGP (Border Gateway Protocol):** Đây là một giao thức định tuyến để truyền tải thông tin giữa các mạng khác nhau. Nó được sử dụng để kết nối các mạng con riêng lẻ thành một mạng lớn hơn, ví dụ như kết nối các mạng của các nhà cung cấp dịch vụ Internet (ISP).
* **ICMP (Internet Control Message Protocol):** Đây là một giao thức được sử dụng để kiểm tra kết nối mạng, tìm kiếm các địa chỉ IP, thông báo lỗi, và đưa ra các thông tin cấu hình cho các thiết bị mạng.

## 2.5. Tầng vận chuyển (Transport Layer)

Tầng Vận chuyển (Transport Layer) là tầng thứ tư trong mô hình OSI và có nhiệm vụ chịu trách nhiệm cho việc truyền tải dữ liệu giữa các tiến trình (process) trên các thiết bị mạng khác nhau. Tầng này sử dụng các giao thức định tuyến để đảm bảo rằng dữ liệu được gửi đúng địa chỉ và đến đúng đích.

Tầng Vận chuyển đảm bảo việc truyền tải dữ liệu một cách tin cậy, có thể được xác nhận và khôi phục nếu có lỗi xảy ra trong quá trình truyền tải. Tầng này cũng quản lý việc đánh số các gói dữ liệu để đảm bảo tính toàn vẹn và độ tin cậy của dữ liệu.

Tầng Vận chuyển cũng cung cấp các cơ chế đa kết nối (multi-connection) để đảm bảo rằng nhiều kết nối mạng có thể được thiết lập và duy trì cùng một lúc/

**Các giao thức phổ biến sử dụng ở tầng Vận chuyển bao gồm:**

* **TCP (Transmission Control Protocol):** Đây là giao thức được sử dụng rộng rãi nhất ở tầng Vận chuyển. TCP đảm bảo việc truyền tải dữ liệu một cách đáng tin cậy, có khả năng xác nhận, phục hồi, và đảm bảo tính toàn vẹn của dữ liệu. Nó cũng sử dụng các cơ chế điều khiển lưu lượng (flow control) và kiểm soát tắc nghẽn (congestion control) để giảm thiểu tắc nghẽn mạng.
* **UDP (User Datagram Protocol):** UDP là một giao thức đơn giản hơn TCP và không đảm bảo tính toàn vẹn và độ tin cậy của dữ liệu. Nó được sử dụng khi việc truyền tải dữ liệu mà không cần quá nhiều kiểm soát và đảm bảo.

## 2.5. Tầng ứng dụng (Application Layer)

Tầng ứng dụng (Application Layer) là tầng cuối cùng trong mô hình OSI và là tầng mà người dùng tương tác trực tiếp khi sử dụng các ứng dụng mạng như trình duyệt web, email, FTP, SSH, Telnet, v.v.

Tầng ứng dụng đóng vai trò quan trọng trong việc định nghĩa giao thức truyền tải dữ liệu giữa các ứng dụng mạng khác nhau. Tầng này cung cấp các dịch vụ và giao thức cho các ứng dụng để chúng có thể trao đổi dữ liệu trên mạng một cách đúng đắn và hiệu quả.

Các giao thức ứng dụng như HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol version 3), IMAP (Internet Message Access Protocol), SSH (Secure Shell) và Telnet được xây dựng trên tầng ứng dụng.

**Một số ví dụ về ứng dụng của Tầng ứng dụng trong thực tế bao gồm:**

* **Truy cập trang web bằng trình duyệt web:** Tầng ứng dụng sử dụng giao thức HTTP để truyền tải các trang web từ máy chủ web đến trình duyệt web.
* **Gửi và nhận email:** Tầng ứng dụng sử dụng giao thức SMTP để gửi email và sử dụng các giao thức POP3 hoặc IMAP để nhận email.
* **Truyền tải tập tin qua mạng:** Tầng ứng dụng sử dụng giao thức FTP để truyền tải các tập tin giữa các máy tính trên mạng.
* **Truyền tải dữ liệu qua mạng bảo mật:** Tầng ứng dụng sử dụng các giao thức bảo mật như SSL và TLS để đảm bảo tính bảo mật của dữ liệu truyền tải trên mạng.

## 2.6. Gia cố hệ thống mạng (network hardening)

Gia cố hệ thống mạng (network hardening) là một phần của gia cố hệ thống đề cập đến quá tăng cường bảo mật của hệ thống mạng đồng thời làm giảm thiểu nguy cơ tấn công từ các mối đe dọa bên ngoài như hacker, malware, .. bằng các biện pháp bảo vệ khác nhau.

### 2.6.1 Gia cố hệ thống tường lửa:

* + 1. **Gia cố vật lý**
       - Kiểm tra hệ thống nguồn điện.
       - Kiểm tra môi trường hoạt động (nhiệt độ, độ ẩm, … ) theo khuyến cáo của nhà sản xuất của các thiết bị.
       - Kiểm tra kết nối mạng.
       - Kiểm tra hệ thống kiểm soát vào-ra.
    2. **Gia cố truy cập từ xa**
       - Tắt các dịch vụ truy cập từ xa không cung cấp kết nối bảo mật (HTTP, Telnet).
       - Cài đặt dịch vụ truy cập từ xa bảo mật (HTTPS, SSH).
       - Hạn chế địa chỉ IP có thể truy cập từ xa với tường lửa.
       - Thiết lập thời gian chờ time-out cho phiên truy cập.
    3. **Gia cố xác thực và phân quyền**
       - Thiết lấp các tính năng mã hóa bảo vệ mật khẩu.
       - Thiết lập hạn chế số lần đăng nhập sai.
       - Tắt chức năng khôi phục mật khẩu.
       - Xóa các tài khoản mặc định, các tài khoản không còn khả dụng.
       - Kiểm tra độ khó của mật khẩu.
       - Cài đặt cơ chế AAA (Authentication – Authorization - Accounting).
    4. **Gia cố tập luật**
       - Hạn chế lưu lượng tới và đi từ tường lửa.
       - Xóa các luật không còn khả dụng.
       - Đảm bảo các luật từ chối một cách rõ ràng tường minh (explicit deny).
    5. **Các gia cố khác**
       - Kích hoạt giao thức Network Time Protocol - NTP để đồng bộ đồng hồ.
       - Gia cố các giao thức định tuyến (RIPv2, OSPF, BGP)
       - Tắt các dihcj vụ không cần thiết (DHCP, ARP Proxy, …)
       - Kích hoạt các mô-đun phát hiện và phòng chống tấn công.
       - Gia cố tính năng nhật ký và ghi log.
       - Kích hoạt cơ chế dự phòng, chịu lỗi.

### 2.6.2 Gia cố Router, Switch

* + 1. **Gia cố vật lý**
    2. **Gia cố truy cập từ xa**
    3. **Gia cố xác thực**
       - Thiết lập tính năng mã hóa bảo vệ mật khẩu.
       - Thiết lập mật khẩu cho kết nối cổng console.
       - Thiết lập mật khẩu cho kết nối Auxiliary – AUX, cổng kết nối điều khiển các thiết bị ngoại vi.
       - Thiết lập mật khẩu cho chế độ quản trị.
    4. **Gia cố các dịch vụ và tính năng**
       - Tắt cá thiệt lập không cần thiết cho phép chuyển tiếp dữ liệu quảng báo.
       - Gia cố dịch vụ SNMP - Simple Network Management Protocol – một giao thức tầng ứng dụng là một phần của Transmission Control Protocol/Internet Protocol (TCP/IP).
       - Tắt các dịch vụ không sử dụng (DHCP, ARP Proxy).
       - Tắt các cổng không sử dụng.
       - Tiển khai cổng loopback.
    5. **Gia cố các tính năng của Router**
       - Thay thế giao thức RIPv1 bằng RIPv2.
       - Gia cố các giao thức định tuyến (OSPF, EIGRP, BGP).
       - Lọc lưu lượng cập nhật thông tin định tuyến.
       - Cài đặt tính năng chống giả mạo IP.
    6. **Gia cố các tính năng của Switch**
       - Tắt default native VLAN không cần thiết.
       - Cài đặt các tính năng chống tấn công giao thức VLAN.
       - Cài đặt các tính năng chống giả mạo ARP, giả mạo địa chỉ Mac.

### 2.6.3 Gia cố WLAN

1. **Gia cố Điểm truy cập (Access Point)**
   * Thay đổi thông tin tài khoản mạc định.
   * Lọc địa chỉ MAC nếu cần.
2. **Giao cố kết nối WLAN**
   * Sử dụng giao thức bảo mật WPA, WPA2.
   * Xóa các tìa khoản không khả dụng khi sử dụng chế độ Doanh nghiệp (Enterprise)

## 2.7 Gia cố ứng dụng

Gia cố ứng dụng cũng là một phần của gia cố hệ thống xoay quanh việc bảo mật ứng dụng được triển khai trên máy chủ.

**Công nghệ thực tế được giúp gia cố ứng dụng hệ thống:**

* + - Phần mềm chống vi-rút (Antivirus software).
    - Phần mềm chống gián điệp (Spyware software).
    - Phần mềm bảo vệ hệ thống khỏi các ứng dụng độc hại (Malware protection application).
    - Hệ thống phát hiện xâm nhập.

# TÀI LIỆU THAM KHẢO

1. Giáo trình môn Mạng máy tính – Đại học Công nghiệp Hà Nội
2. Network Security Essentials: Applications and Standards - William Stallings.
3. https://www.geeksforgeeks.org/osi-security-architecture/
4. https://vi.wikipedia.org/wiki/M%C3%B4\_h%C3%ACnh\_OSI
5. https://en.wikipedia.org/wiki/OSI\_model