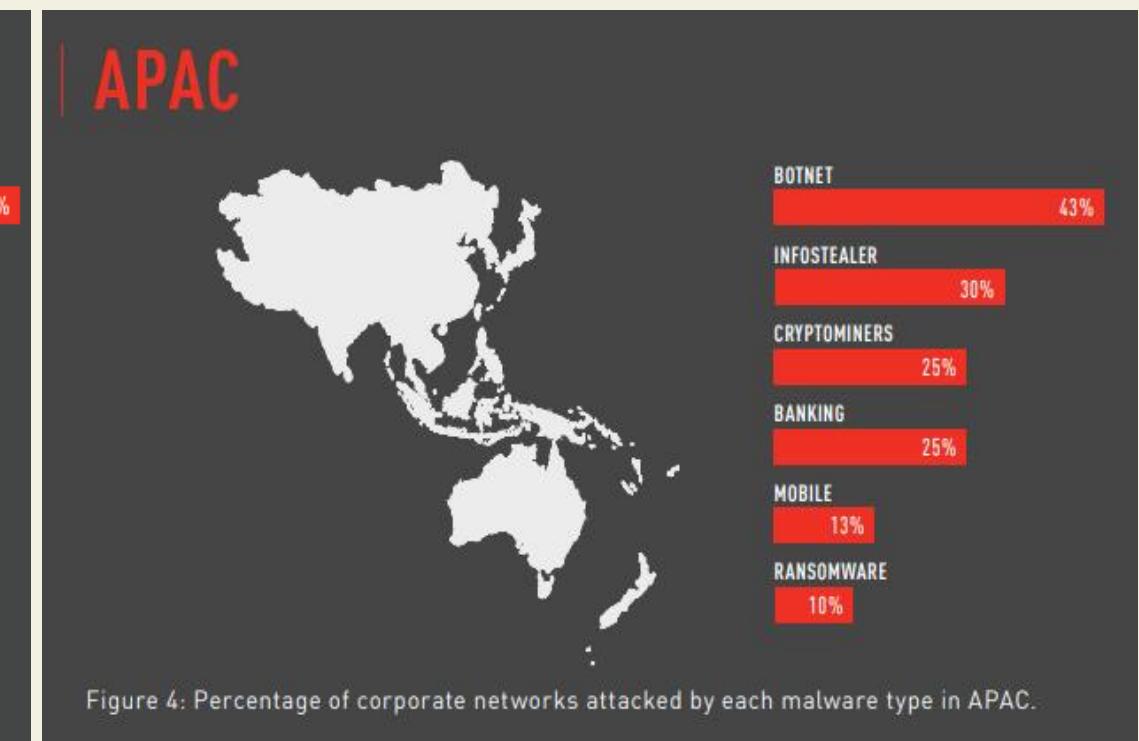
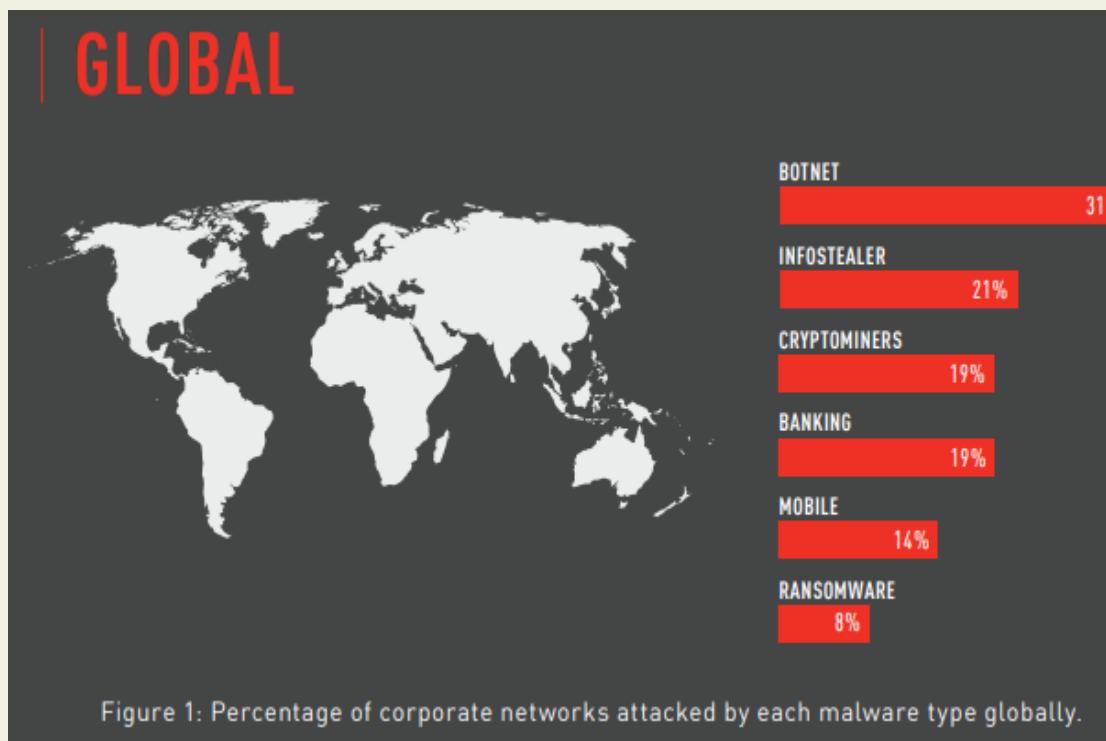


- Tổng quan an ninh mạng
- Thuật toán mã hóa khóa bí mật và công khai (LT+TH)
- An ninh tầng giao vận (LT+TH)
- An ninh thư điện tử (LT+TH)
- An ninh IP
- An ninh mạng không dây (LT+TH)
- Các mô hình mạng an toàn và phần mềm độc hại (LT+TH)
- Thâm nhập trái phép và tường lửa (LT+TH)

0.1. Một số thống kê về tình hình an ninh mạng

Một số thống kê về An ninh mạng trong báo cáo “Security Report 01/24/22” của hãng bảo mật Checkpoint.

Năm 2021, tổng các cuộc tấn công vào các mạng doanh nghiệp tăng 50% mỗi tuần so với năm 2020.



0.1. Một số thống kê về tình hình an ninh mạng

Một số thống kê về An ninh mạng trong báo cáo “Security Report 01/24/22” của hãng bảo mật Checkpoint.

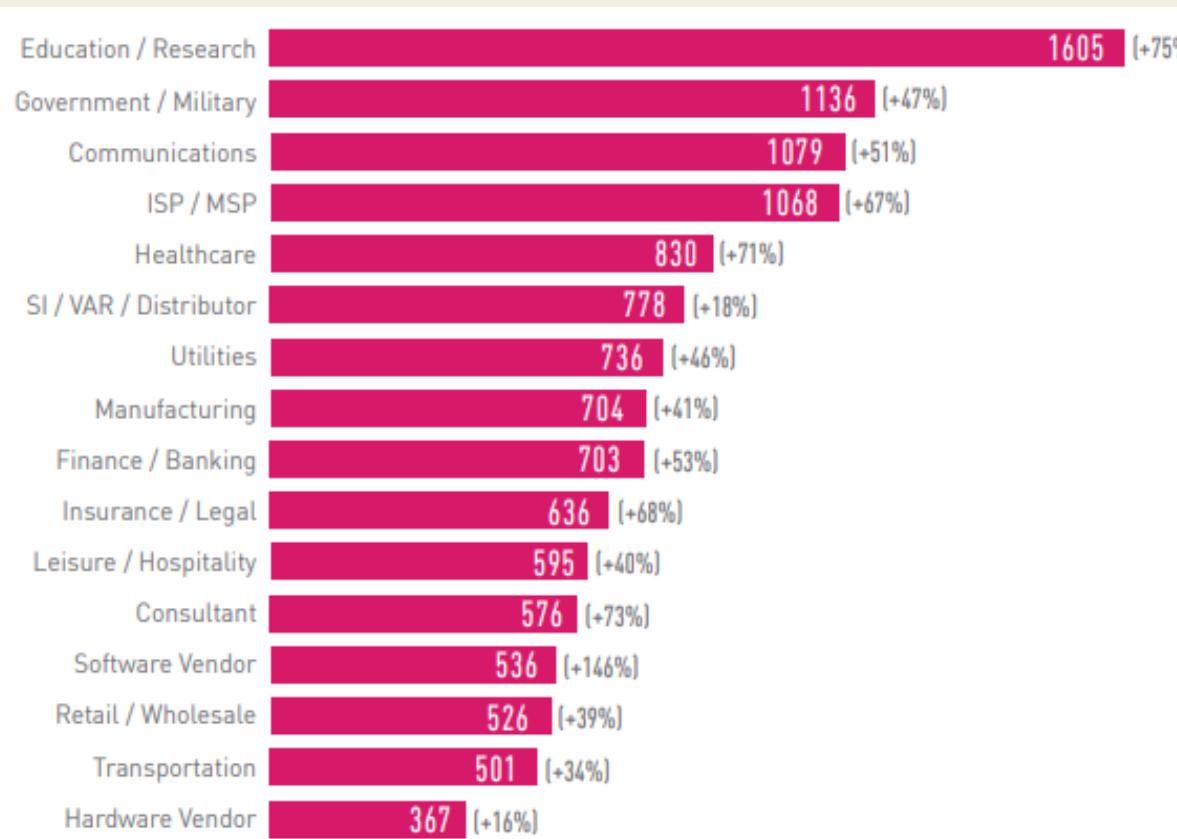
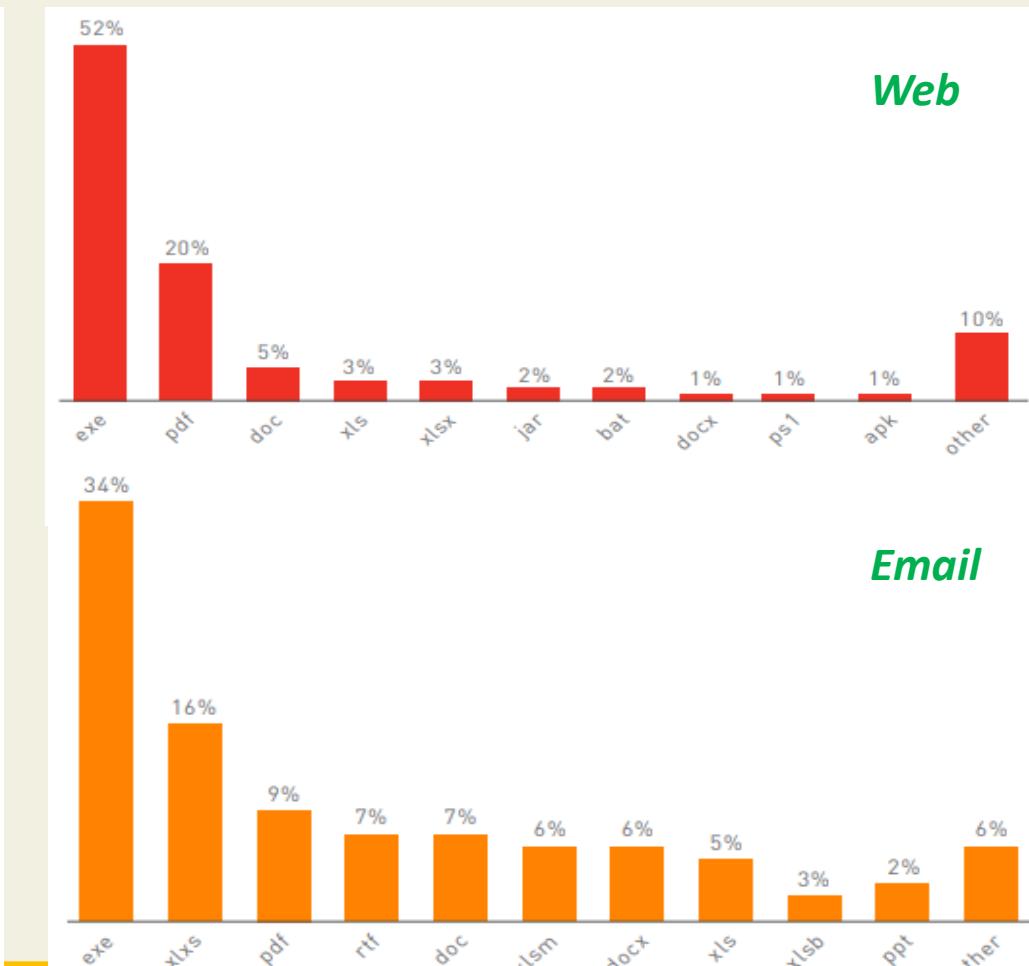
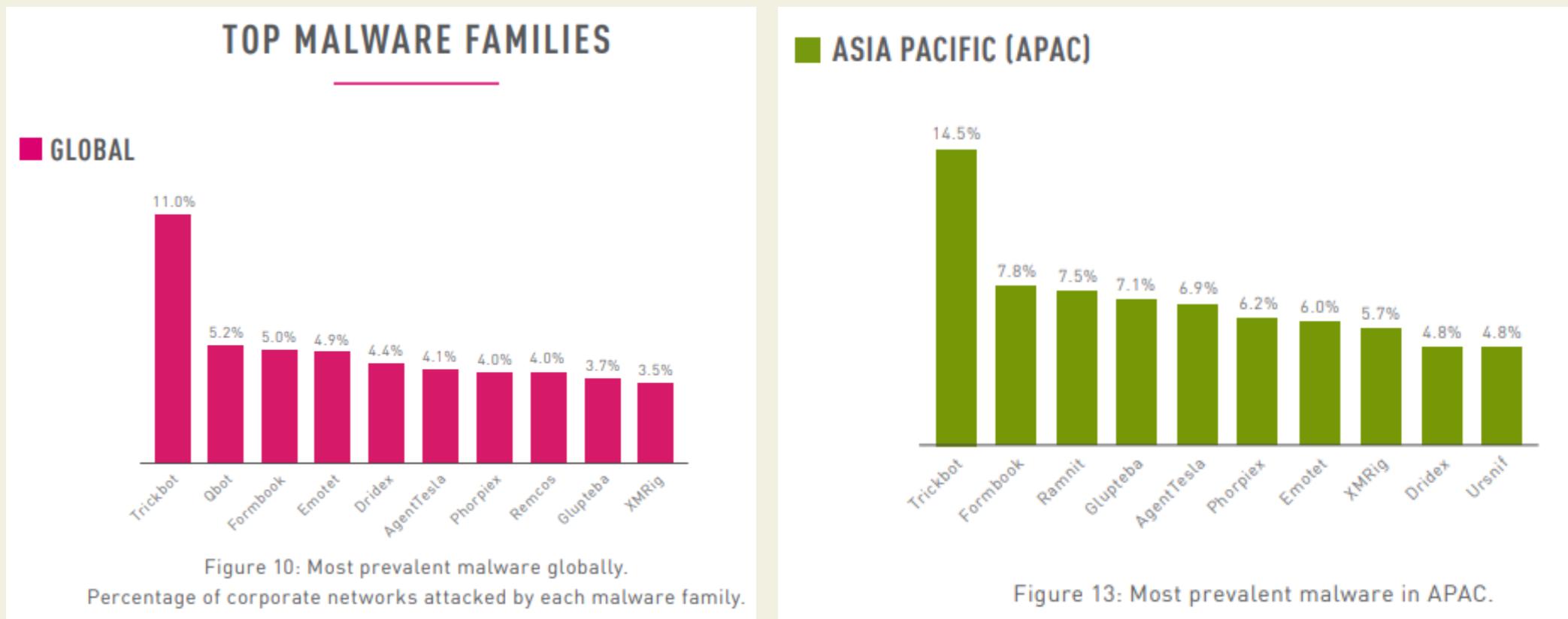


Figure 6: Average weekly attacks per organization by Industry 2021, compared to 2020.



0.1. Một số thống kê về tình hình an ninh mạng

Dữ liệu về mã độc được lấy từ bản đồ mối đe dọa trên mạng toàn cầu của Checkpoint từ tháng 1 đến tháng 12 năm 2021 của hãng: <https://threatmap.checkpoint.com/>



0.1. Một số thống kê về tình hình an ninh mạng

Việt Nam: Luật An ninh mạng được Quốc hội thông qua năm 2018 và chính thức có hiệu lực từ 01/01/2019, với 7 chương, 43 điều quy định về hoạt động bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội trên không gian mạng, bên cạnh đó là trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. (tập trung điều 2, 8, 19, 41, 42)



Số máy tính Việt Nam bị nhiễm 5 dòng mã độc phổ biến năm 2022

Năm 2022, thiệt hại do mã độc máy tính gây ra đối với người dùng Việt Nam ở mức 21,2 nghìn tỷ (tương đương 883 triệu USD) → Mức thiệt hại nhóm thấp so với thế giới (tổng cầu 1000 tỷ USD).

Lần đầu tiên sau hơn 10 năm Bkav thực hiện thống kê, con số thiệt hại ghi nhận giảm so với các năm trước đó.

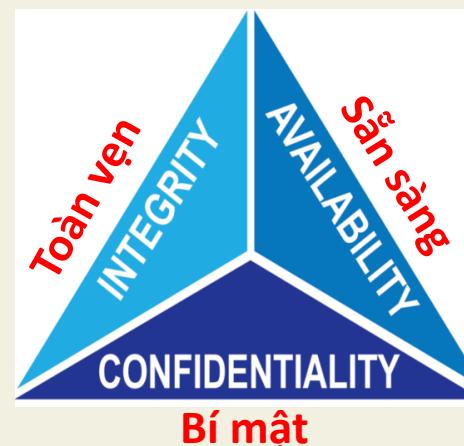
Việt Nam tăng 25 bậc về chỉ số an toàn an ninh mạng GCI, cho thấy nỗ lực của Chính phủ và giới an ninh mạng trong nước.

I. Tổng quan về an ninh mạng

1.1. Giới thiệu chung về an ninh mạng máy tính

Một số định nghĩa quan trọng:

- **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).
- **An ninh mạng máy tính:** Sự bảo vệ dành cho hệ thống thông tin tự động nhằm đạt được các mục tiêu đó là duy trì tính toàn vẹn, tính sẵn sàng (tính khả dụng) và tính bí mật của tài nguyên hệ thống thông tin (bao gồm phần cứng, mềm, phần sun, thông tin/dữ liệu và viễn thông).



Hình 1. Tam giác CIA

Ba nguyên tắc cốt lõi này
phải dẫn đường cho tất cả
các hệ thống an ninh mạng

1.1. Giới thiệu chung về an ninh mạng máy tính

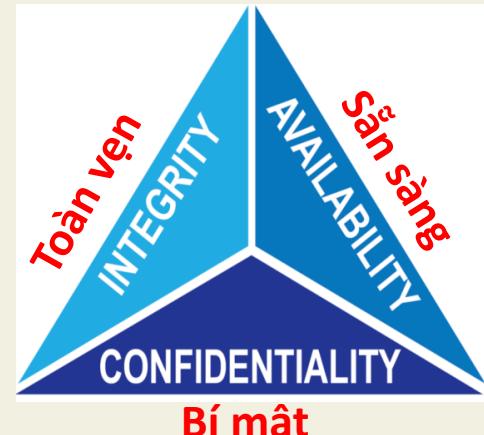
Tính bí mật: là sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. Gồm 2 nội dung là Bí mật về dữ liệu và Quyền riêng tư.

→ Đối với an ninh mạng thì tính bí mật rõ ràng là điều đầu tiên được nói đến và nó thường xuyên bị tấn công nhất.

Tính toàn vẹn: Là sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó Bảo đảm sự chính xác về dữ liệu và hệ thống. Gồm có toàn vẹn về dữ liệu và toàn vẹn của hệ thống:

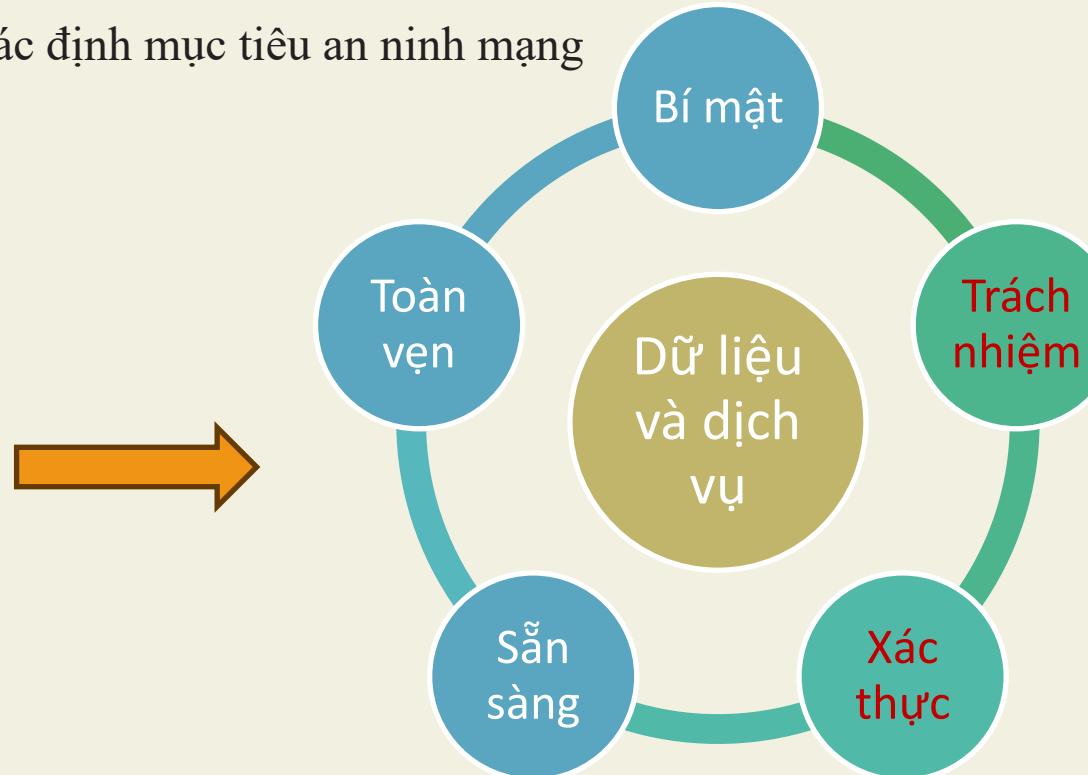
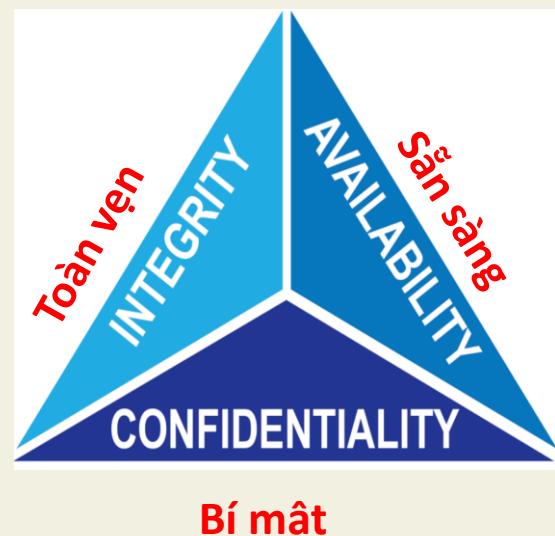
- Toàn vẹn dữ liệu: Đảm bảo rằng dữ liệu và các chương trình chỉ được thay đổi theo bởi người được cấp quyền.
- Tính toàn vẹn của hệ thống: Đảm bảo rằng một hệ thống thực hiện chức năng dự kiến của nó một cách nguyên vẹn, không bị thao túng trái phép một cách có chủ ý hoặc vô ý.

Tính sẵn sàng: Đảm bảo truy cập và sử dụng thông tin kịp thời và đáng tin cậy. Mất tính sẵn sàng là sự gián đoạn truy cập hoặc gián đoạn sử dụng thông tin hoặc gián đoạn sử dụng hệ thống thông tin.



1.1. Giới thiệu chung về an ninh mạng máy tính

Một bức tranh hoàn chỉnh để xác định mục tiêu an ninh mạng được đề xuất gồm 5 yếu tố:



Trách nhiệm: Mục tiêu an ninh quy định các hành động của một thực thể phải được quy một cách duy nhất về thực thể đó. Điều này hỗ trợ chống từ chối, ngăn chặn, cách ly lỗi, phát hiện và ngăn chặn xâm nhập, phục hồi sau hành động và hành động pháp lý.

Tính xác thực: Thể hiện thuộc tính được xác minh và có độ tin cậy; độ tin cậy vào tính hợp lệ của việc truyền thông, tin nhắn hoặc người khởi tạo tin nhắn

1.1. Giới thiệu chung về an ninh mạng máy tính

Một số thách thức an ninh mạng máy tính:

- Lĩnh vực Bảo mật không đơn giản, và nhất là đối với những người mới lần đầu tiếp cận
- Khi phát triển một cơ chế hoặc thuật toán bảo mật cụ thể, phải luôn xem xét các cuộc tấn công tiềm ẩn vào các tính năng bảo mật đó
- Thủ tục để cung cấp các dịch vụ bảo mật là phức tạp và không giống nhau, phải xem xét các khía cạnh khác nhau của các mối đe dọa thì các cơ chế bảo mật mới có ý nghĩa
- Vị trí thiết kế, sử dụng các cơ chế bảo mật.
- Cơ chế bảo mật không dừng lại chỉ một thuật toán hay một giao thức cụ thể, cũng có thể yêu cầu các thông tin bí mật như khóa mã hóa, các cách thức nâng cao bảo mật,...
- Cuộc đấu trí giữa kẻ tấn công và người thiết kế hệ thống hay quản trị viên
- Còn chưa nhận thức rõ mức độ nguy hại khi chưa bị tấn công
- ...

I. Tổng quan về an ninh mạng

1.2. Kiến trúc an ninh OSI (Open System Interconnection)

Kiến trúc an ninh OSI xác định cách tiếp cận có hệ thống để cung cấp các giải pháp bảo mật ở mỗi lớp, từ đó xác định các cơ chế và dịch vụ an ninh có thể được sử dụng mở mỗi lớp trong mô hình 7 lớp OSI nhằm bảo mật dữ liệu truyền qua mạng.

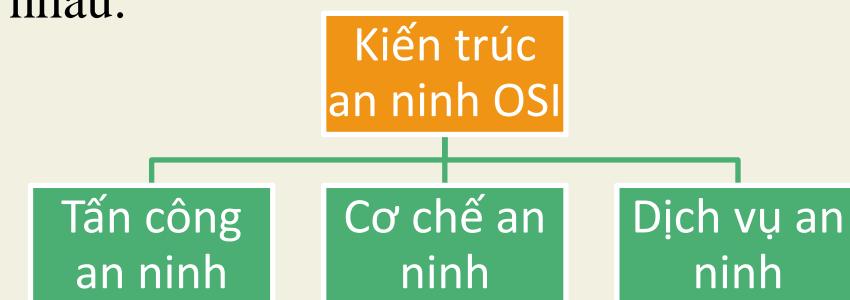
Các cơ chế và dịch vụ an ninh này sẽ giúp đảm bảo tính CIA của dữ liệu



I. Tổng quan về an ninh mạng

1.2. Kiến trúc an ninh OSI (Open System Interconnection)

- **Tấn công an ninh (security attacks):** được định nghĩa là bất kỳ hành động nào mà tổn hại đến tính an toàn của thông tin thuộc sở hữu bởi một tổ chức.
- **Cơ chế an ninh (security mechanics):** Một quy trình (hoặc một thiết bị kết hợp với một quy trình) mà được thiết kế để phát hiện, ngăn chặn hoặc khắc phục một tấn công an toàn.
- **Dịch vụ an ninh (security services):** Một dịch vụ xử lý hoặc truyền thông giúp tăng cường bảo mật cho các hệ thống xử lý dữ liệu và truyền dữ liệu của một tổ chức. Các dịch vụ bảo mật nhằm chống lại các cuộc tấn công bảo mật và có thể sử dụng một hoặc nhiều cơ chế bảo mật khác nhau.



I. Tổng quan về an ninh mạng

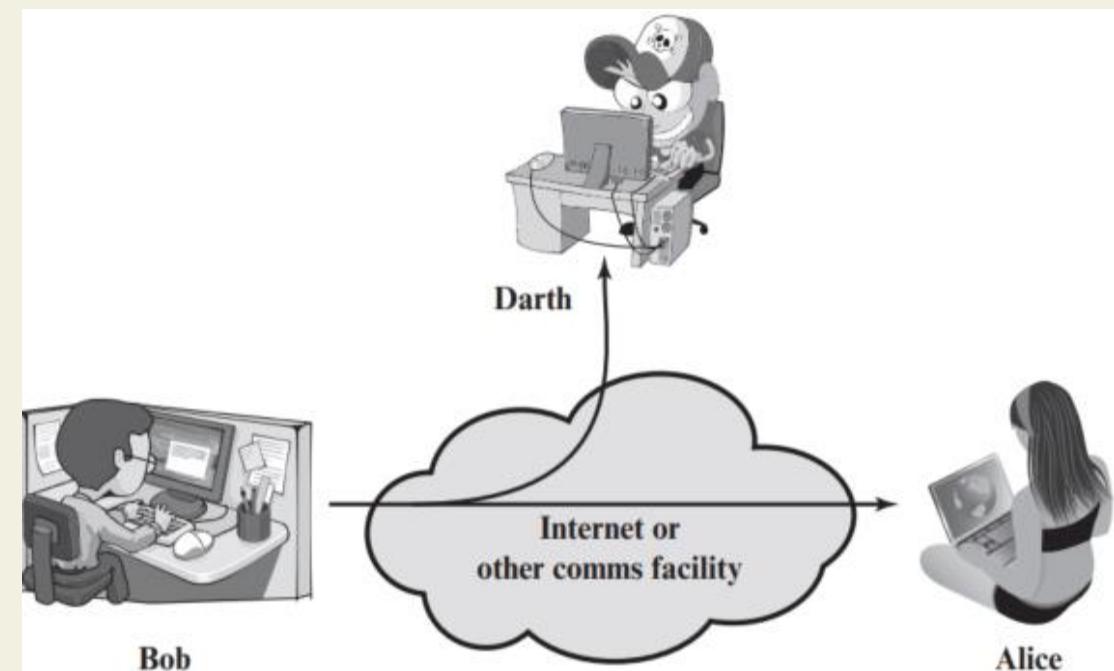
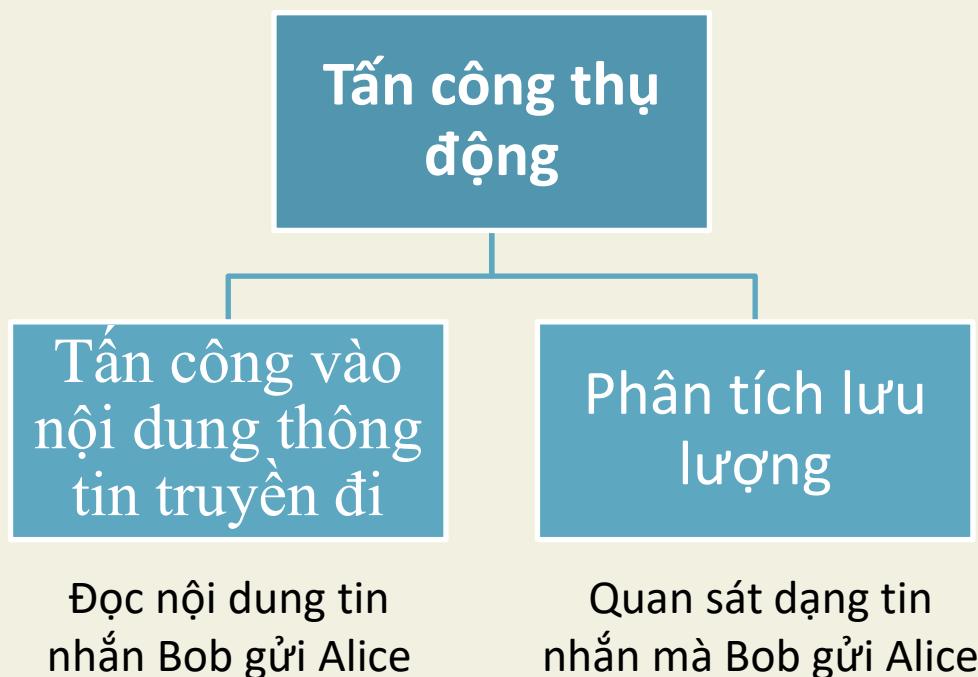
1.3. Tấn công an ninh

Có 2 loại hình tấn công an ninh chính được sử dụng trong cả X.800 (đây là kiến trúc bảo mật cho hệ thống OSI được ITU quy định), tiêu chuẩn RFC 4949 (RFC viết tắt của Request for comment, bao gồm các thuật ngữ bảo mật Internet).

- **Tấn công thụ động:** là cuộc tấn công cố gắng tìm hiểu hoặc sử dụng thông tin từ hệ thống nhưng không ảnh hưởng đến tài nguyên của hệ thống.
- **Tấn công chủ động:** là cuộc tấn công mà attacker cố gắng thay đổi tài nguyên hệ thống hoặc ảnh hưởng đến hoạt động của các hệ thống đó

I. Tổng quan về an ninh mạng

Tấn công thụ động: Các cuộc tấn công bị động có bản chất là nghe lén hoặc giám sát đường truyền dữ liệu. Mục tiêu là lấy được thông tin đang được truyền đi.

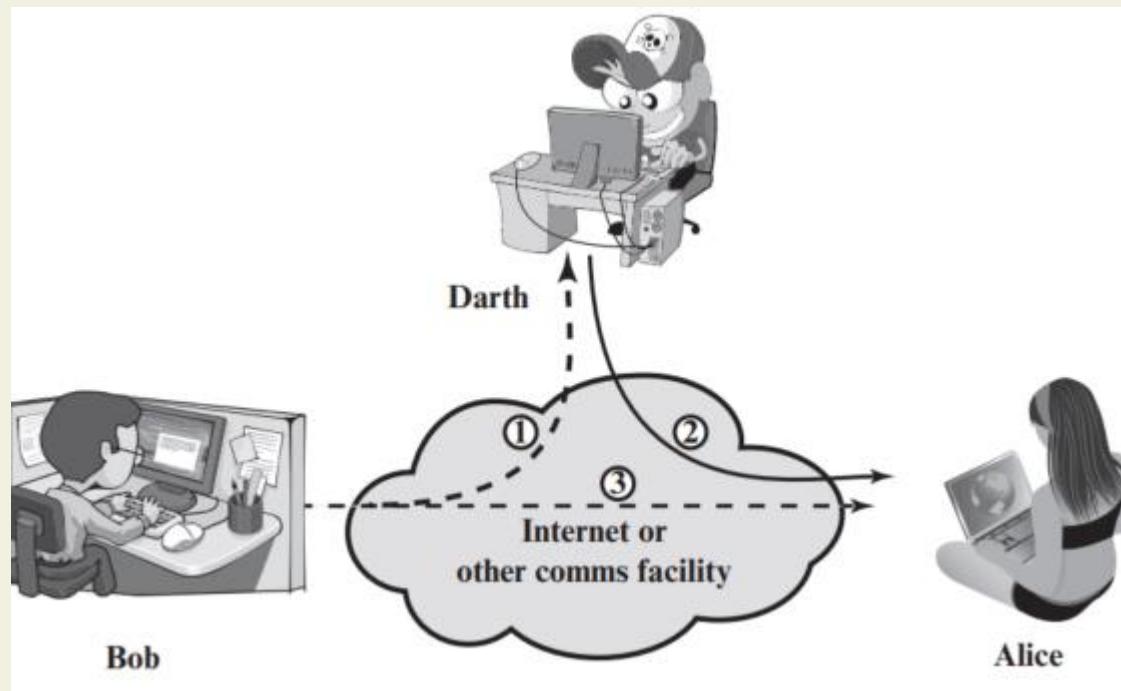


Các cuộc tấn công thụ động rất khó phát hiện do không tạo ra sự thay đổi gì về dữ liệu

Để đối phó với các cuộc tấn công này, chúng ta phải có các kỹ thuật phòng ngừa (như mã hóa) hơn là phát hiện.

I. Tổng quan về an ninh mạng

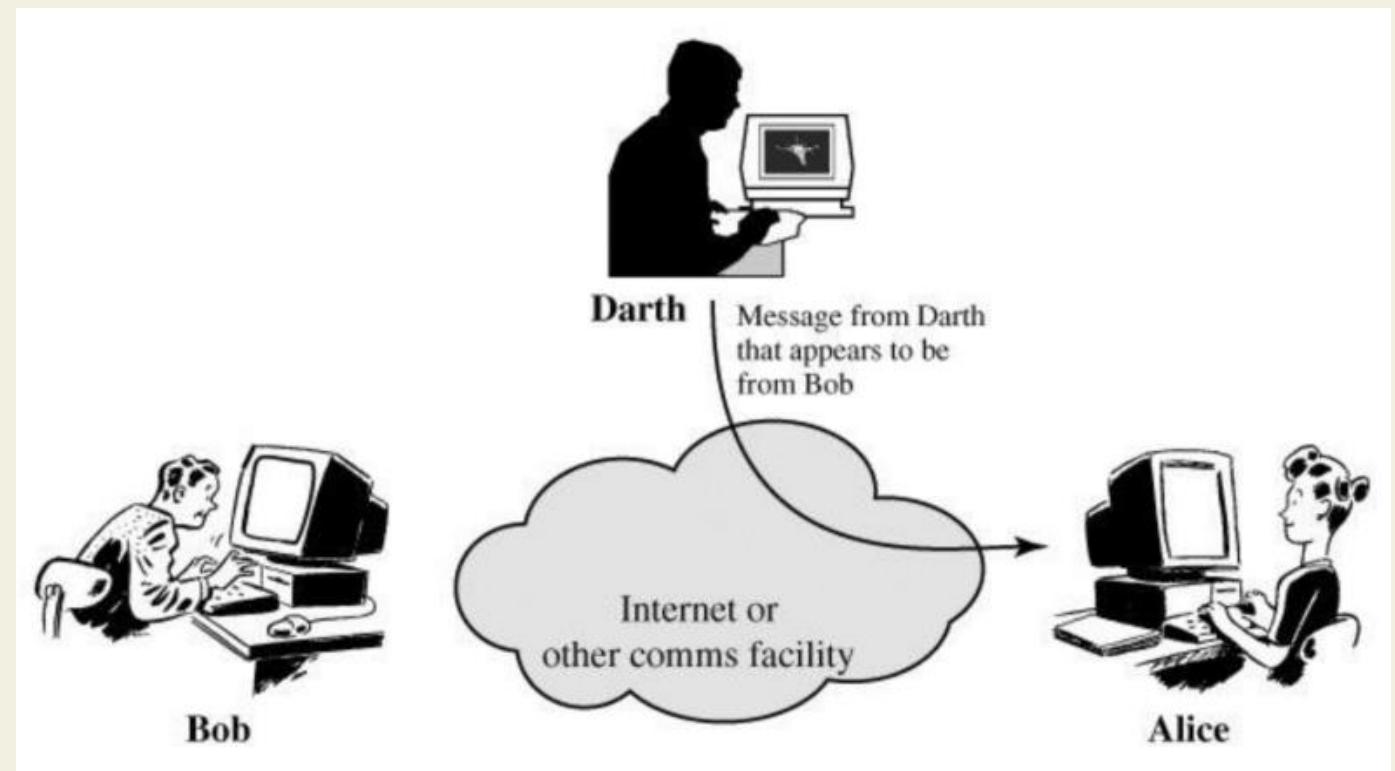
Tấn công chủ động: liên quan đến việc sửa đổi luồng dữ liệu hoặc tạo luồng giả và có thể được chia thành 4 loại: giả mạo, phát lại, sửa đổi thông tin, và từ chối dịch vụ.



I. Tổng quan về an ninh mạng

Tấn công chủ động

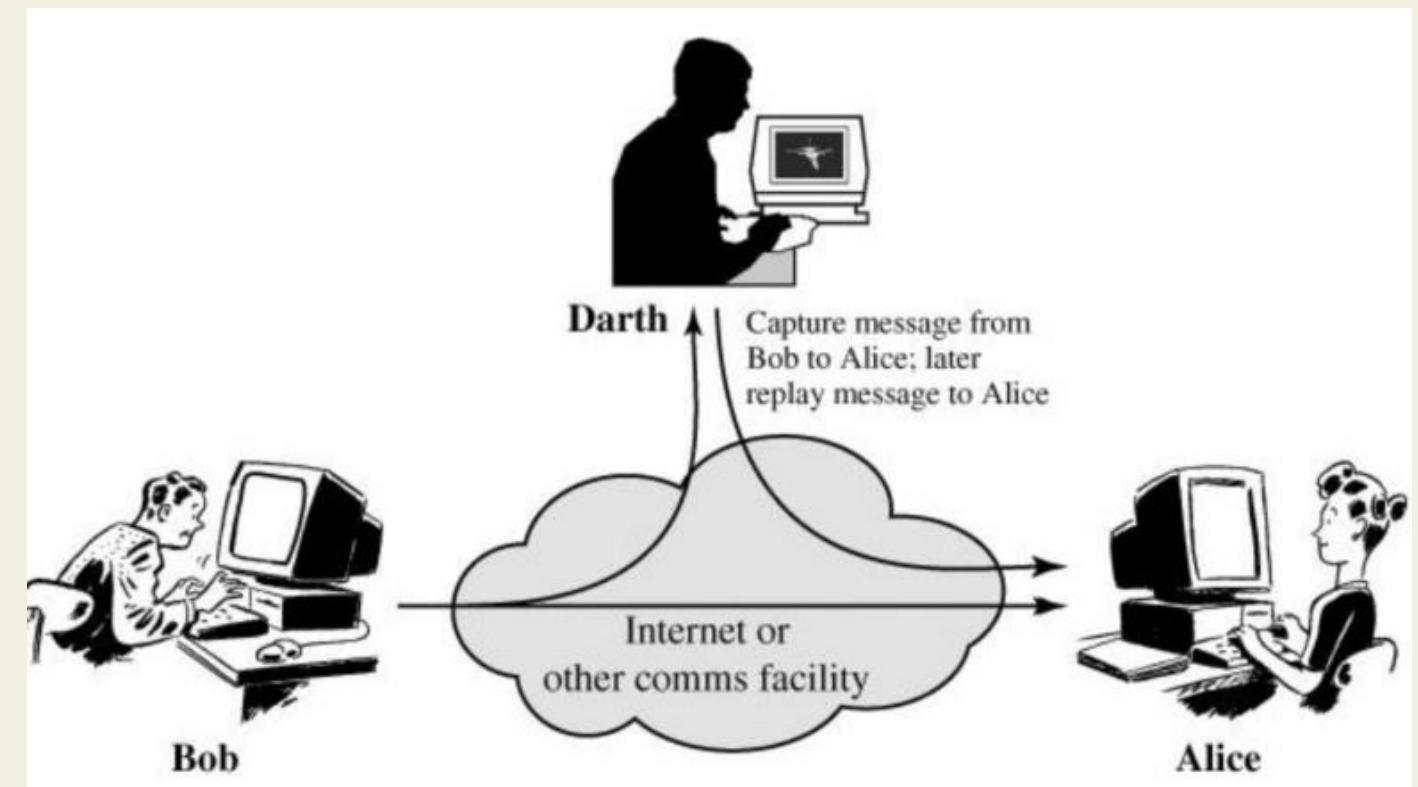
Giả mạo: Diễn ra khi một thực thể giả vờ một thực thể khác (2) – tin nhắn từ Darth tới Alice nhưng lại giả vờ là từ Bob



I. Tổng quan về an ninh mạng

Tấn công chủ động

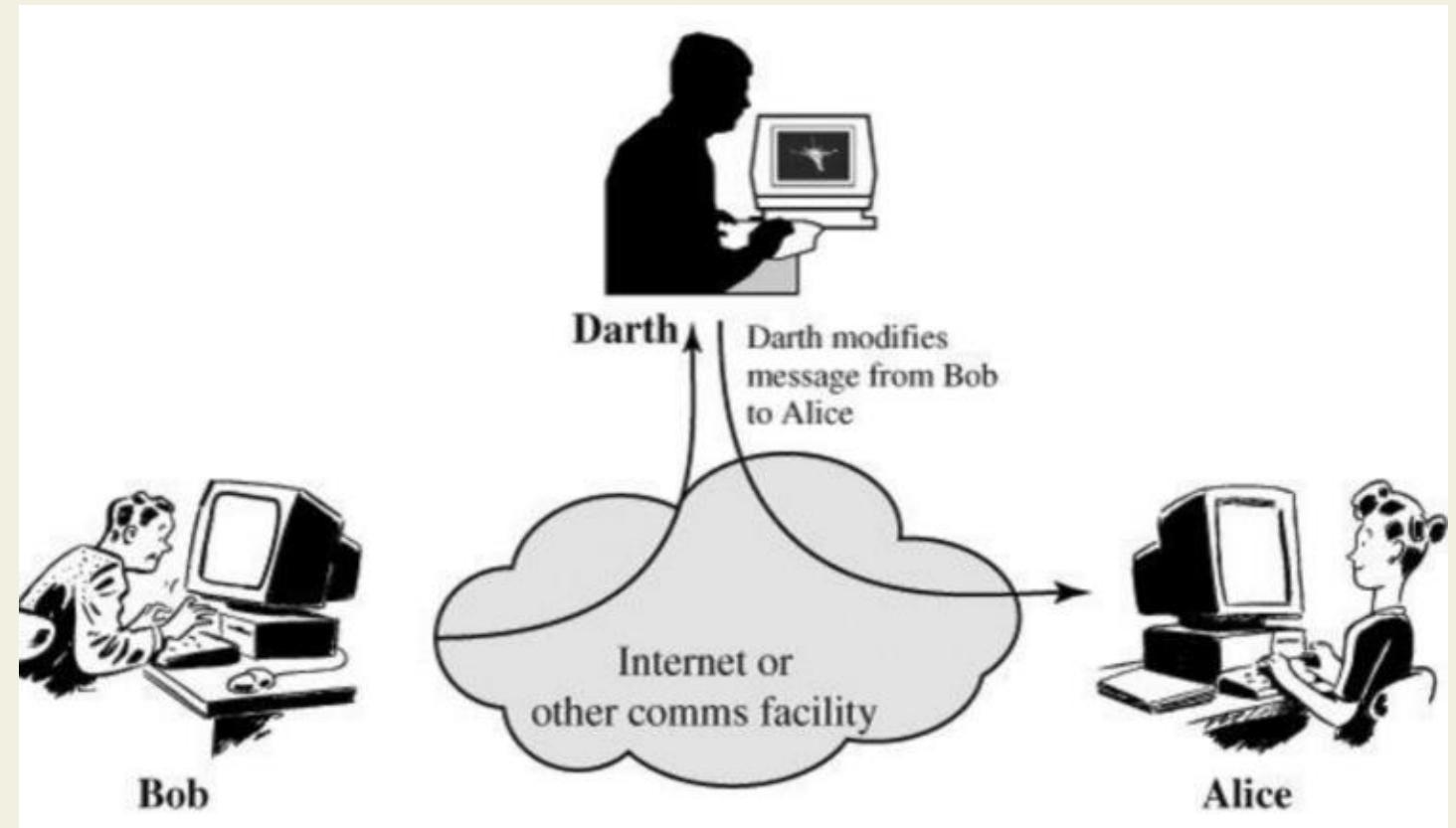
- **Phát lại:** Liên quan đến việc nắm bắt thụ động dữ liệu và truyền lại sau đó tạo ra hiệu ứng không xác thực (1,2,3) – Darth bắt gói tin từ Bob tới Alice; sau đó phát lại tin nhắn tới Alice



I. Tổng quan về an ninh mạng

Tấn công chủ động

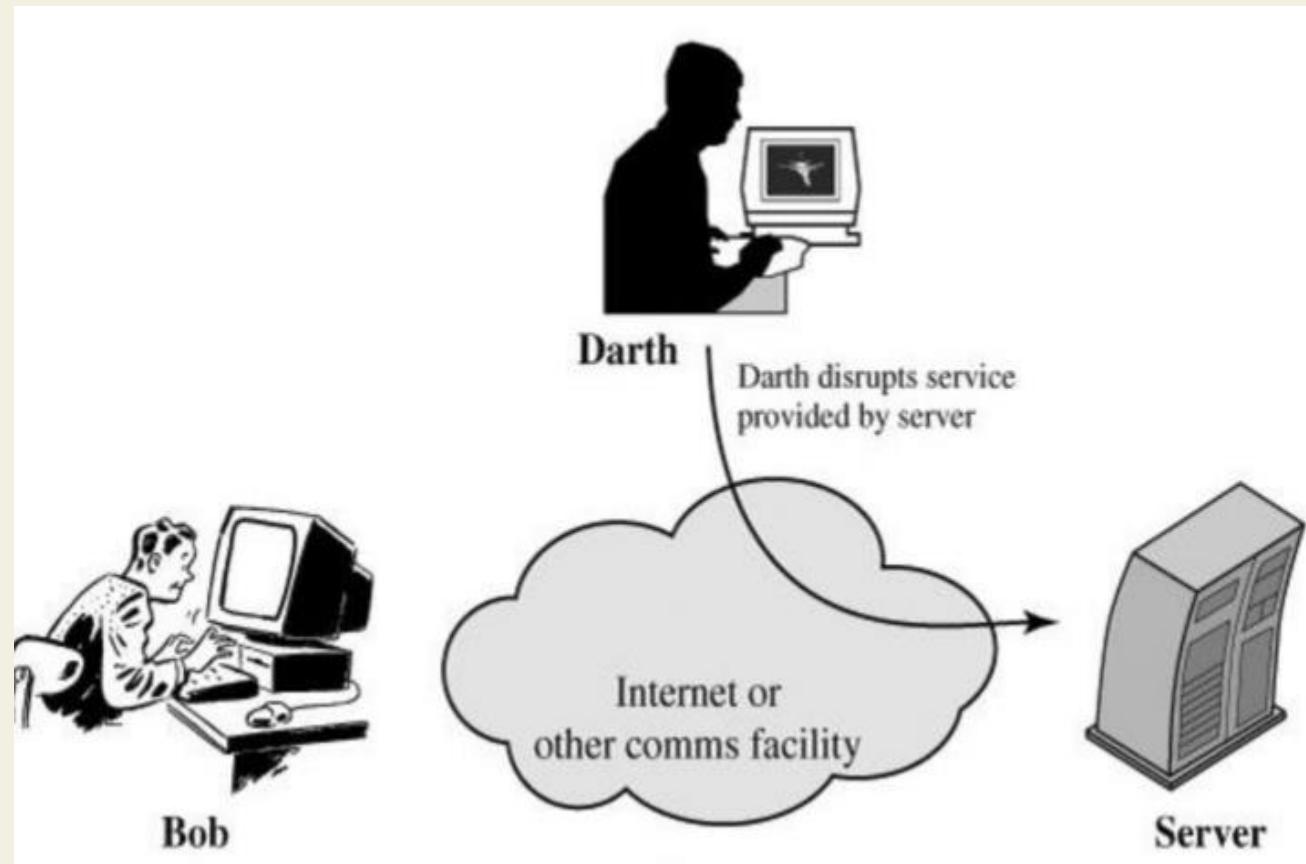
- Sửa đổi: tin nhắn bị sửa lại một phần hoặc tin nhắn gửi đi bị trễ để tạo ra hiệu ứng không xác thực (1, 2) – Darth sửa tin nhắn mà Bob gửi cho Alice.



I. Tổng quan về an ninh mạng

Tấn công chủ động

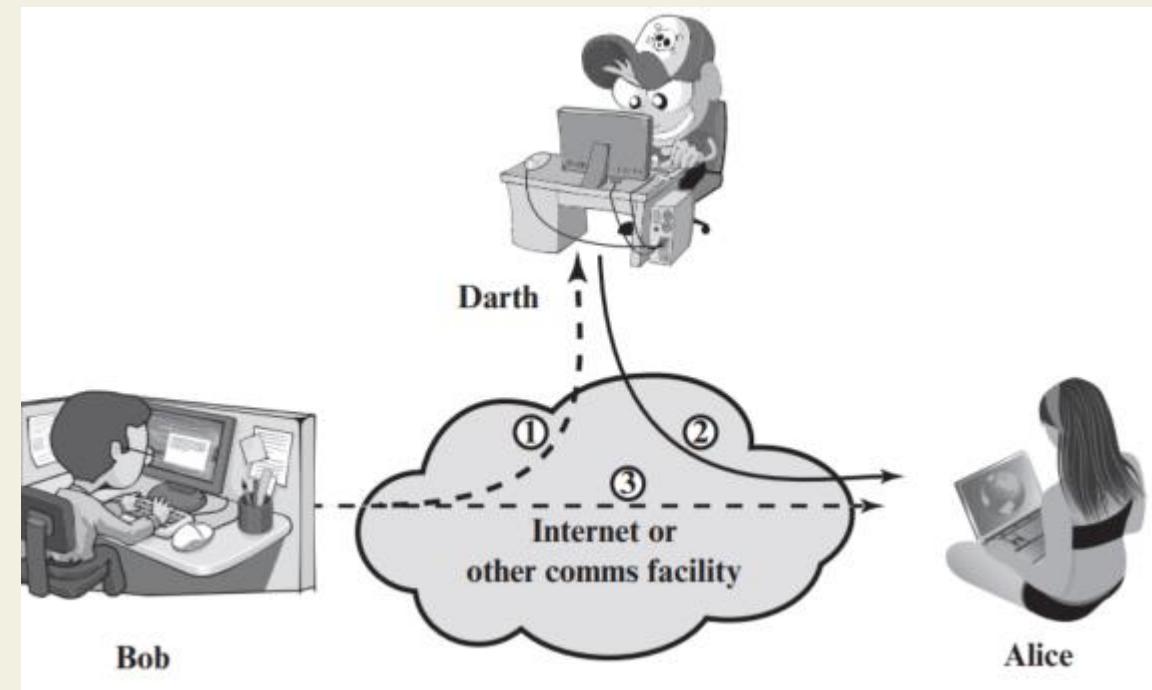
- **Tùy chối dịch vụ:** là ngăn chặn hoặc cản trở việc sử dụng hoặc quản lý các phương tiện truyền thông (3 – Darth sẽ ngắt dịch vụ được cung cấp bởi máy chủ).



I. Tổng quan về an ninh mạng

Tấn công chủ động:

- Các cuộc tấn công chủ động thể hiện các đặc điểm ngược lại của các tấn công bị động.
- Có rất nhiều lỗ hổng vật lý, phần mềm và mạng tiềm ẩn → rất khó để ngăn chặn hoàn toàn tấn công chủ động
- Mục tiêu là phát hiện các cuộc tấn công chủ động và khắc phục sự cố



I. Tổng quan về an ninh mạng

1.3. Dịch vụ an ninh

- **X.800** định nghĩa dịch vụ an ninh là một dịch vụ mà được cung cấp bởi một lớp giao thức của các hệ thống mở truyền thông, đảm bảo bảo mật đầy đủ cho hệ thống hoặc truyền dữ liệu.
- Trong **RFC 4949** cũng trình bày một định nghĩa khá rõ ràng về dịch vụ bảo mật đó là dịch vụ xử lý hoặc truyền thông được tạo ra bởi hệ thống để cung cấp một loại bảo vệ cụ thể các tài nguyên của hệ thống; dịch vụ bảo mật thực hiện sẽ các chính sách bảo mật được tạo ra từ các cơ chế bảo mật.

X.800 đã chia các dịch vụ an ninh này thành 5 loại và 14 dịch vụ cụ thể



I. Tổng quan về an ninh mạng

1.3. Dịch vụ an ninh

Xác thực: Đảm bảo thực thể truyền thông là đáng tin cậy.

- (1) Xác thực thực thể ngang hàng: cung cấp chứng thực định danh của thực thể ngang hàng trong một liên kết
 - Hai thực thể được coi là ngang hàng nếu chúng triển khai cùng một giao thức trong các hệ thống khác nhau, ví dụ 2 mô-đun TCP trong hai hệ thống giao tiếp.
 - Xác thực thực thể ngang hàng được cung cấp để sử dụng khi thiết lập hoặc đổi mới trong giai đoạn truyền dữ liệu của kết nối. Nó cố gắng cung cấp sự tin cậy rằng một thực thể không thực hiện giả mạo hoặc phát lại trái phép kết nối trước đó.
- (2) Xác thực nguồn gốc dữ liệu: dùng trong truyền dẫn phi kết nối chứng thực nguồn của dữ liệu.
 - Nó không cung cấp khả năng bảo vệ để chống lại sự sao chép hoặc sửa đổi dữ liệu.
 - Loại dịch vụ này hỗ trợ các ứng dụng như thư điện tử, nơi mà không có sự tương tác trước giữa các thực thể giao tiếp.

I. Tổng quan về an ninh mạng

1.3. Dịch vụ an ninh

Điều khiển truy cập

- Ngăn chặn việc sử dụng trái phép tài nguyên (nghĩa là dịch vụ này kiểm soát ai có quyền truy cập vào tài nguyên).
- Trong bối cảnh an ninh mạng, kiểm soát truy cập là khả năng giới hạn và kiểm soát quyền truy cập vào các hệ thống máy chủ và ứng dụng thông qua các liên kết truyền thông.

I. Tổng quan về an ninh mạng

1.3. Dịch vụ an ninh

- **Bảo mật dữ liệu:** Là việc bảo vệ dữ liệu để không bị tiết lộ một cách trái phép, tức là bảo vệ dữ liệu được truyền đi từ các cuộc tấn công thụ động.
 - (1) Bảo mật kết nối – là việc bảo vệ dữ liệu người dùng trên một kết nối;
 - (2) Bảo mật không kết nối – việc bảo mật tất cả dữ liệu người dùng trong một khối dữ liệu đơn;
 - (3) Bảo mật trường dữ liệu có chọn lọc – bảo mật các trường dữ liệu được chọn trong dữ liệu người dùng trên một kết nối hoặc trong một khối dữ liệu đơn;
 - (4) Bảo mật luồng lưu lượng – bảo mật thông tin thu được từ việc quan sát các luồng lưu lượng.

I. Tổng quan về an ninh mạng

1.3. Dịch vụ an ninh

Tính toàn vẹn của dữ liệu: đảm bảo rằng dữ liệu nhận được chính xác như khi được gửi bô một thực thể được xác thực (nghĩa là dữ liệu không bị sửa đổi, chèn, xóa hoặc phát lại).

- (1) Tính toàn vẹn của kết nối với khôi phục – cung cấp tính toàn vẹn của tất cả dữ liệu người dùng trên một kết nối hoặc phát hiện mọi chỉnh sửa, chèn, xóa hoặc phát lại của bất kì dữ liệu nào trong toàn bộ chuỗi dữ liệu với nỗ lực khôi phục;
- (2) Tính toàn vẹn của kết nối không cần khôi phục – tương tự nhưng chỉ cung cấp khả năng phát hiện mà không khôi phục;
- (3) Tính toàn vẹn có kết nối của các trường dữ liệu có chọn lọc – cung cấp tính toàn vẹn của các trường dữ liệu được chọn trong khối dữ liệu người dùng được truyền thông qua một kết nối và xác định xem các trường này có bị sửa đổi, chèn, xóa hay phát lại hay chưa;
- (4) Tính toàn vẹn của phi kết nối – cung cấp tính toàn vẹn của một khối dữ liệu phi kết nối đơn và có thể ở dạng phát hiện sự sửa đổi dữ liệu;
- (5) Tính toàn vẹn phi kết nối trường dữ liệu có chọn lọc – cung cấp tính toàn vẹn của các trường đã chọn trong một khối dữ liệu phi kết nối và có thể ở dạng phát hiện sự sửa đổi dữ liệu có hay không.

I. Tổng quan về an ninh mạng

1.3. Dịch vụ an ninh

- **Tính chối bỏ:** cung cấp sự bảo vệ chống lại việc từ chối bởi một trong những thực thể tham gia vào một phần hoặc tất cả một giao tiếp truyền thông, có nghĩa là dịch vụ này ngăn người gửi hoặc người nhận từ chối một bản tin đã được truyền đi. Bao gồm:
 - (1) tính chối bỏ nguồn gốc – cung cấp bằng chứng rằng bản tin đã được gửi bởi bên được chỉ định;
 - (2) Chống chối bỏ đích đến – cung cấp bằng chứng rằng bên được chỉ định đã nhận được bản tin.

I. Tổng quan về an ninh mạng

1.5. Các cơ chế an ninh

- Theo X.800, các cơ chế an ninh được chia thành những cơ chế mà hoạt động ở từng lớp giao thức cụ thể, như ở lớp ứng dụng của mô hình TCP/IP, những cơ chế này không dành riêng cho bất kỳ lớp giao thức hoặc dịch vụ an ninh nào.

Cơ chế an ninh chuyên biệt: có thể được tích hợp vào một lớp giao thức để cung cấp một số dịch vụ an ninh của mô hình OSI.
Gồm có:

- Mã hóa
- Chữ ký số
- Kiểm soát truy cập
- Độn lưu lượng
- Điều khiển định tuyến
- Công chứng

Cơ chế an ninh phổ quát: các cơ chế này không dành riêng cho bất kỳ lớp giao thức hoặc dịch vụ bảo mật OSI cụ thể nào.

Gồm có:

- Chức năng đáng tin cậy
- Nhãn an ninh
- Phát hiện sự kiện
- Dấu kiểm tra an ninh
- Kiểm toán an ninh
- Khôi phục an ninh

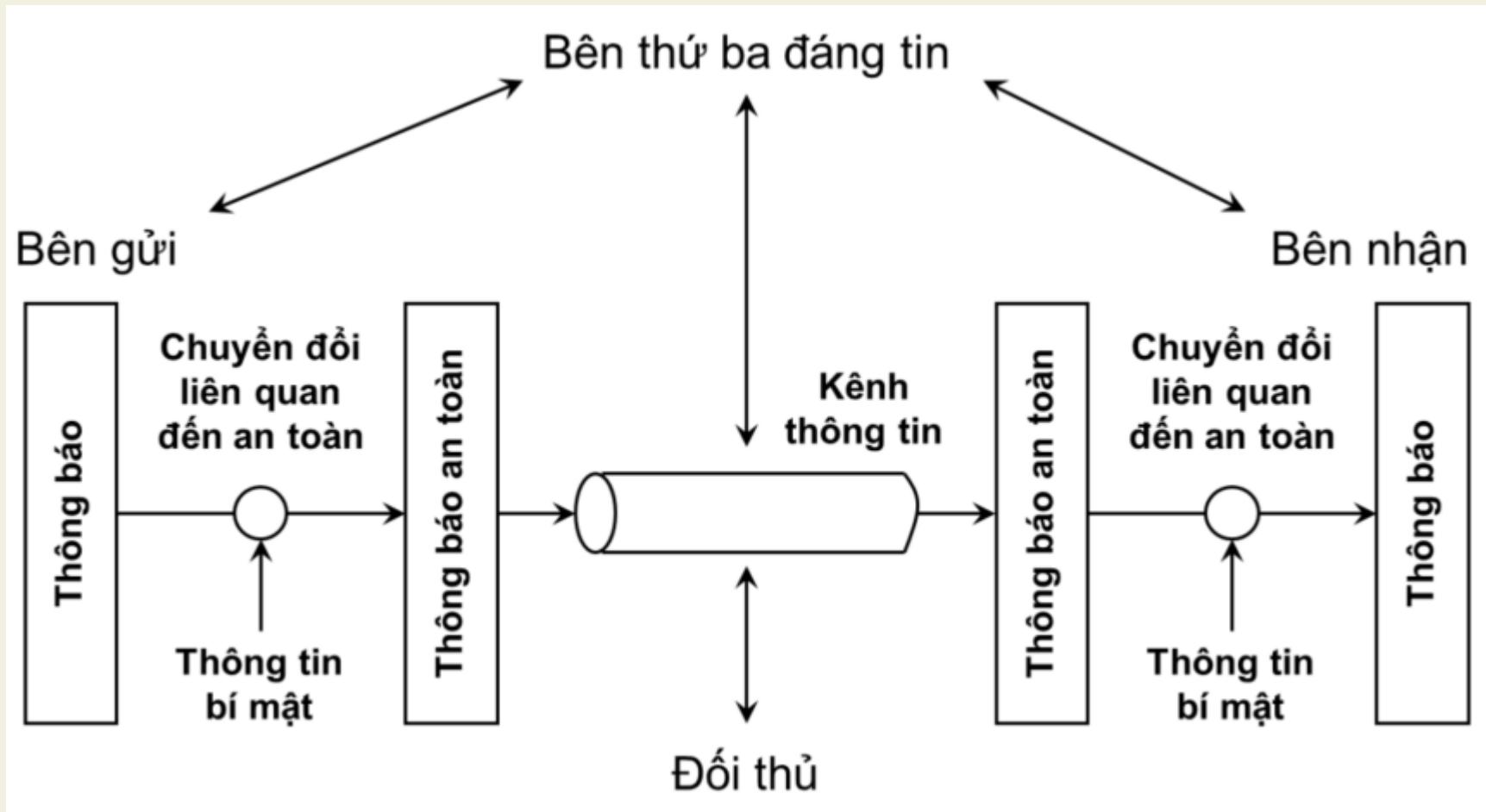
I. Tổng quan về an ninh mạng

- Mối quan hệ giữa Dịch vụ an ninh và Các cơ chế an ninh

Service	Mechanism							
	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y				Y	Y		
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

I. Tổng quan về an ninh mạng

1.5. Mô hình mạng an toàn



I. Tổng quan về an ninh mạng

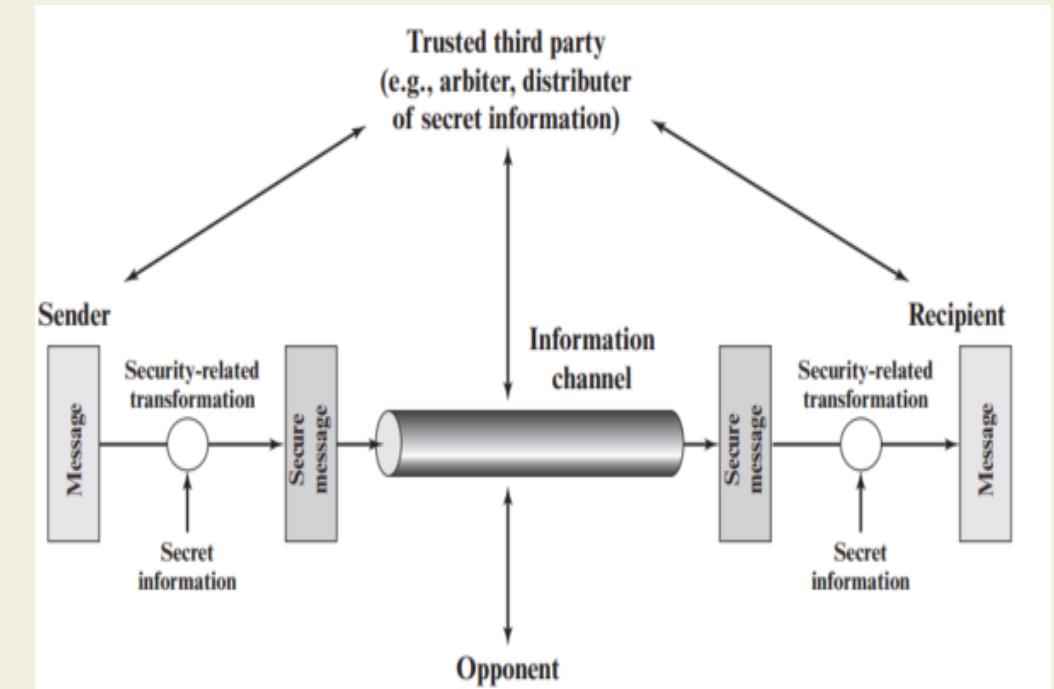
1.5. Mô hình mạng an toàn

- Các khía cạnh an ninh phát huy tác dụng khi cần thiết hoặc mong muốn bảo vệ việc truyền dẫn thông tin khỏi những kẻ có thể gây ra mối đe dọa đối với tính bảo mật, tính xác thực,...
- Tất cả các kỹ thuật cung cấp tính an ninh, an toàn đều có 2 thành phần:
 1. Chuyển đổi liên quan đến bảo mật thông tin được gửi đi. Ví dụ như mã hóa tin nhắn, làm xáo trộn tin nhắn để kẻ tấn công không thể đọc được, và thêm mã dựa vào nội dung của tin nhắn, mã này có thể được sử dụng để xác định danh tính người gửi.
 2. Một số thông tin bí mật được chia sẻ bởi 2 chủ thể trao đổi thông tin, và người ta hi vọng những kẻ tấn công không thể biết được thông tin này. Ví dụ là khóa mã hóa được sử dụng cùng phép biến đổi để xáo trộn tin nhắn trước khi gửi tin nhắn đi và giải mã tin nhắn bên nhận.

I. Tổng quan về an ninh mạng

1.5. Mô hình mạng an toàn

- Một bên thứ ba đáng tin cậy cũng cần thiết để tăng thêm sự an toàn trong quá trình truyền thông tin.
- Ví dụ, trong trao đổi thông tin giữa Bob và Alice, một bên thứ ba sẽ chịu trách nhiệm phân phối thông tin bí mật cho Bob và Alice và bảo vệ để không tiết lộ thông tin đó cho kẻ nghe lén.
- Hoặc một bên thứ ba sẽ đóng vai trò là người phân xử các tranh chấp giữa hai bên liên quan đến tính xác thực của việc truyền thông tin.

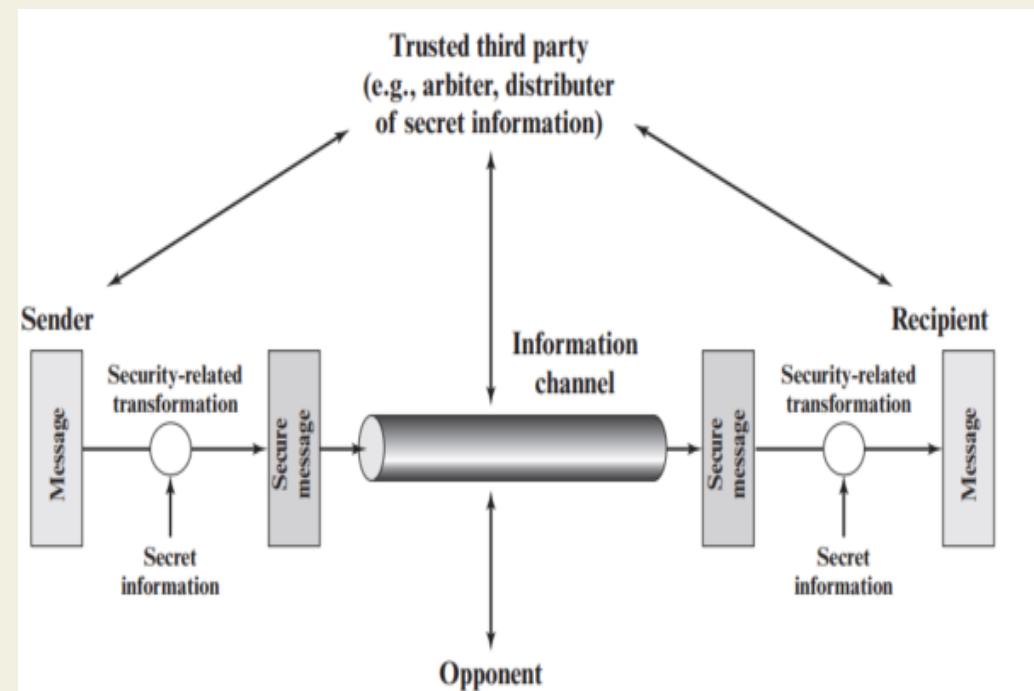


I. Tổng quan về an ninh mạng

1.5. Mô hình mạng an toàn

4 nhiệm vụ cơ bản trong thiết kế một dịch vụ an ninh cụ thể:

1. Thiết kế một thuật toán để thực hiện chuyển đổi thông tin liên quan đến bảo mật. Thuật toán phải đủ mạnh để cho kẻ tấn công không thể “đánh bại” được.
2. Tạo thông tin bí mật được sử dụng với thuật toán
3. Phát triển các phương pháp phân phối và chia sẻ thông tin bí mật này.
4. Chỉ định một giao thức để việc sử dụng thuật toán bảo mật và thông tin bí mật đạt được một dịch vụ an ninh, an toàn cụ thể.



1.5. Mô hình mạng an toàn

- Có hai mối nguy cơ đối với các chương trình trên máy tính gồm có:
 1. Các nguy cơ truy cập thông tin: Người truy cập trái phép chặn bắt hoặc sửa đổi dữ liệu.
 2. Các nguy cơ về dịch vụ: Khai thác các lỗ hổng dịch vụ trên máy tính để ngăn cản người dùng hợp pháp sử dụng.
- Các cơ chế an ninh cần thiết để đối phó với các truy cập trái phép được chia thành hai loại chính
 1. Gatekeeper: bao gồm các quy trình đăng nhập dựa trên mật khẩu, được thiết kế để từ chối quyền truy cập đối với những người dùng trái phép.
 2. Tuyến phòng thủ thứ hai bao gồm các giải pháp bảo mật để phát hiện sự hiện diện của những kẻ xâm nhập trái phép. Những vấn đề này sẽ được đề cập ở những chương tiếp theo.

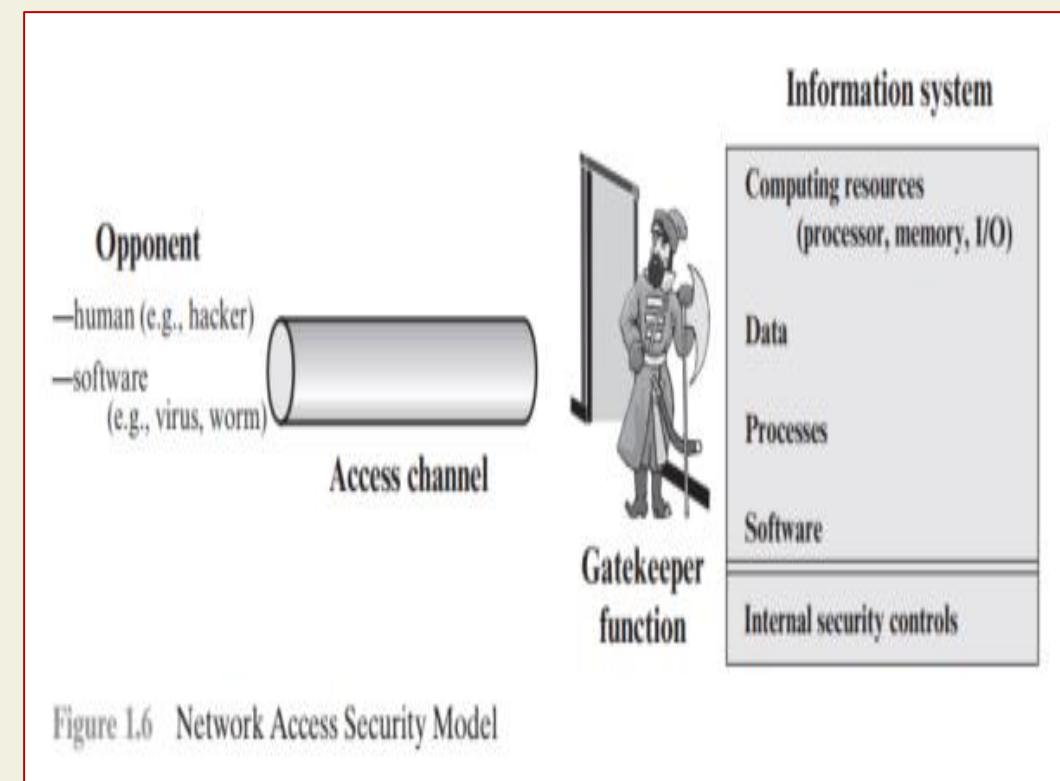


Figure 1.6 Network Access Security Model

I. Tổng quan về an ninh mạng

Câu hỏi ôn tập

- Câu hỏi 1: Trình bày kiến trúc an ninh OSI?
- Câu hỏi 2: Trình bày các dịch vụ an ninh theo X.800?
- Câu hỏi 3: Tại sao tấn công thụ động lại khó phát hiện và các tấn công chủ động lại khó ngăn chặn?

Câu hỏi vấn đề:

- Câu 1: Hãy xem xét một máy rút tiền tự động ATM, trong đó người dùng cung cấp số nhận dạng cá nhân PIN (personal identification number) và một thẻ rút ngân hàng để truy cập. Hãy lấy ví dụ về các yêu cầu về tính bảo mật, toàn vẹn và tính sẵn sàng liên quan đến hệ thống.
- Câu 2: Hãy xác định mức độ tác động (thấp, trung bình, cao) cho các hệ thống dưới đây khi 3 yếu tố bảo mật, tính toàn vẹn, tính sẵn sàng (khả dụng) bị mất. Giải thích vì sao lại xác định mức độ như vậy?
 1. Cổng thông tin của Chính phủ để cung cấp các thông tin cho các tổ chức, đơn vị, dịch vụ của Chính phủ.
 2. Một bệnh viện quản lý hồ sơ y tế của bệnh nhân
 3. Một tổ chức tài chính quản lý thông tin hành chính thông thường (không phải thông tin liên quan đến quyền riêng tư)
 4. Trung tâm Khảo thí của một trường Đại học lưu trữ các dữ liệu về các kì thi, chặng hạn như các câu hỏi của các kỳ thi sắp tới, bảng điểm, và thông tin chi tiết về người chấm thi.

MÃ HÓA

Nội dung chính:

Giới thiệu chung về mật mã học và thám mã

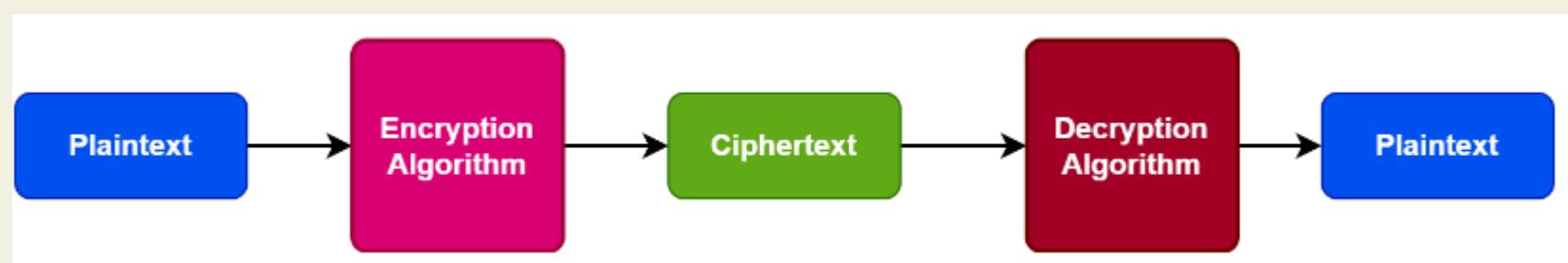
Mã hóa bí mật

Mã hóa công khai

Chữ ký số điện tử

1. Giới thiệu chung về mật mã học (Cryptography)

- Mật mã học là một lĩnh vực liên quan đến các kỹ thuật ngôn ngữ và toán học để đảm bảo an toàn thông tin, cụ thể là trong thông tin liên lạc.
- Mật mã học gắn liền với quá trình mã hóa tức là chuyển đổi thông tin từ dạng "có thể hiểu được" thành dạng "không thể hiểu được" hay chuyển đổi thông tin từ “bản rõ – plain text” sang “bản mã – cipher text” và ngược lại là quá trình giải mã



1. Giới thiệu chung về mật mã học (Cryptography)

Mật mã học giúp bảo đảm các yếu tố sau cho dữ liệu:

- **Tính bí mật (confidentiality):** thông tin chỉ được tiết lộ cho những ai được phép
- **Tính toàn vẹn (integrity):** thông tin không thể bị thay đổi mà không bị phát hiện.
- **Tính xác thực (authentication):** người gửi (hoặc người nhận) có thể chứng minh đúng họ.
- **Tính chống chối bỏ (non-repudiation):** người gửi hoặc nhận sau này không thể chối bỏ việc đã gửi hoặc nhận thông tin.

1. Giới thiệu chung về mật mã học (Cryptography)

- **Phân loại:**

- Loại thao tác dùng để chuyển bản rõ thành bản mã: thay thế, chuyển vị
- Số khóa sử dụng: Khóa đơn –khóa bí mật (Mã hóa đối xứng); và Hai khóa – Khóa công khai (Mã hóa bất đối xứng)
- Cách xử lý bản rõ: Mã hóa khối và mã hóa luồng



Mã hóa đối xứng



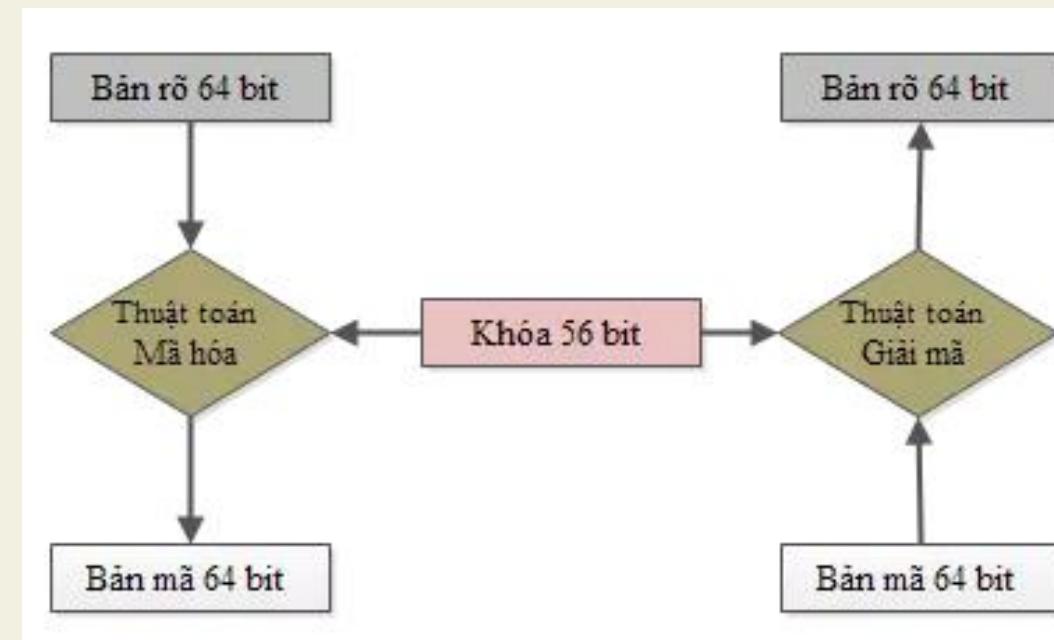
Mã hóa bất đối xứng

2. Thám mã (cryptanalysis)

- Thám mã hay còn gọi là phân tích mật mã – đây là ngành học nghiên cứu các phương thức để thu được ý nghĩa của thông tin đã được mã hóa
- Các phương pháp tấn công thám mã:
 - Tìm khóa vét cạn
 - Phân tích thống kê
 - Phân tích toán học

2.1. Mật mã DES (Data Encryption Standard)

- Ngày 13/5/1973 ủy ban quốc gia về tiêu chuẩn của Mỹ công bố yêu cầu về mật mã áp dụng cho toàn quốc → sự ra đời của DES
- Ban đầu DES được phát triển từ hệ mã Lucifer bởi công ty IBM, năm 1975
- Sau đó DES được xem như là chuẩn mã hóa dữ liệu cho các ứng dụng

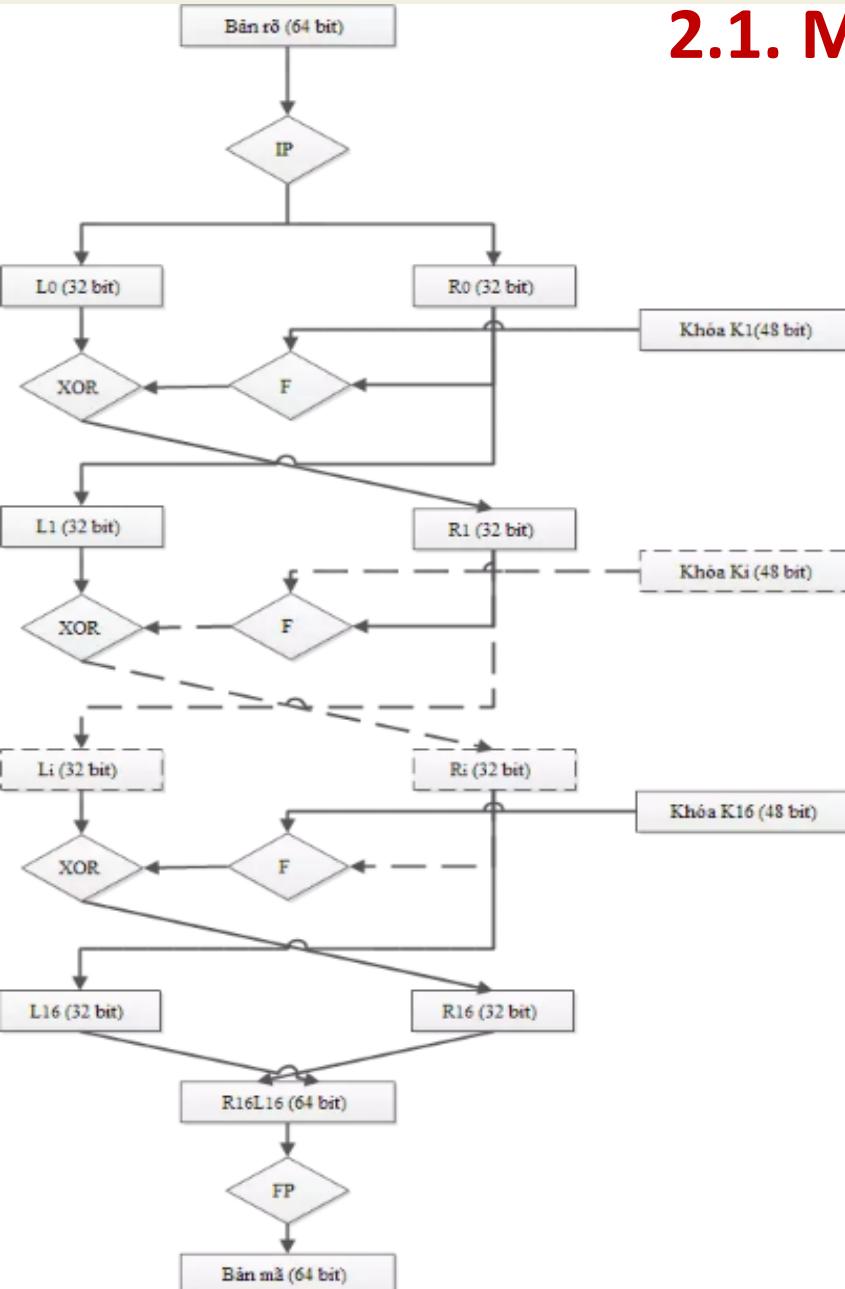


2.3. Mật mã DES (Data Encryption Standard)

- **Đặc điểm của thuật toán DES như sau:**
- DES là một thuật toán mã hóa khối, độ dài mỗi khối là 64 bít
- Khóa dùng trong DES có độ dài toàn bộ 64 bít. Tuy nhiên chỉ có 56 bít thực sự được sử dụng, 8 bít còn lại chỉ dùng cho việc kiểm tra
- DES xuất ra bản mã 64 bít
- Thuật toán thực hiện 16 vòng lặp, chỉ khác nhau về khóa trong mỗi vòng lặp đó
- Mã hóa và giải mã được sử dụng cùng một khóa

2.1. Mật mã DES (Data Encryption Standard)

- **Sơ đồ khái quát thuật toán DES**
- Với mỗi khóa K và bản rõ x, quá trình lập mã diễn ra như sau:
 - Ban đầu, dùng một phép hoán vị IP (Initial Permutation), từ x với 64 bít sẽ biến thành một từ mới $IP(x)$, từ này được chia thành 2 nửa L_0 và R_0 , mỗi nửa là một từ 32 bít
 - Từ cặp (L_0, R_0) sẽ dùng 15 lần những phép toán giống nhau để liên tiếp được các cặp $(L_1, R_1), \dots, (L_{15}, R_{15})$, sau đó dùng phép hoán vị nghịch đảo IP^{-1} cho từ đảo ngược $R_{15}L_{15}$ ta sẽ được bản mã y tương ứng.



2.1. Mật mã DES (Data Encryption Standard)

- Thông tin đầu vào là 64 bít, được chia thành 2 khối trái (L) và phải (R)
- Từ khóa 56 bít tạo ra các khóa con (subkey) gọi là K_i .
- Hàm f là một hàm hoán vị
- Trong quá trình mã hóa, dữ liệu đầu vào phải thực hiện quá trình hoán vị đầu IP (initial permutation) và hoán vị cuối (final permutation) sau vòng thứ 16
- Hàm cơ sở f cho phép đảm bảo tính bảo mật trong DES
- Cấu trúc vòng lặp DES thực hiện theo công thức sau:

$$(L_i, R_i) = (R_{i-1}, L_{i-1}) \text{ XOR } f(R_{i-1}, K_i)$$

- Trong đó (L_i, R_i) là nửa trái và nửa phải lấy được của phép biến đổi vòng lặp thứ i

II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

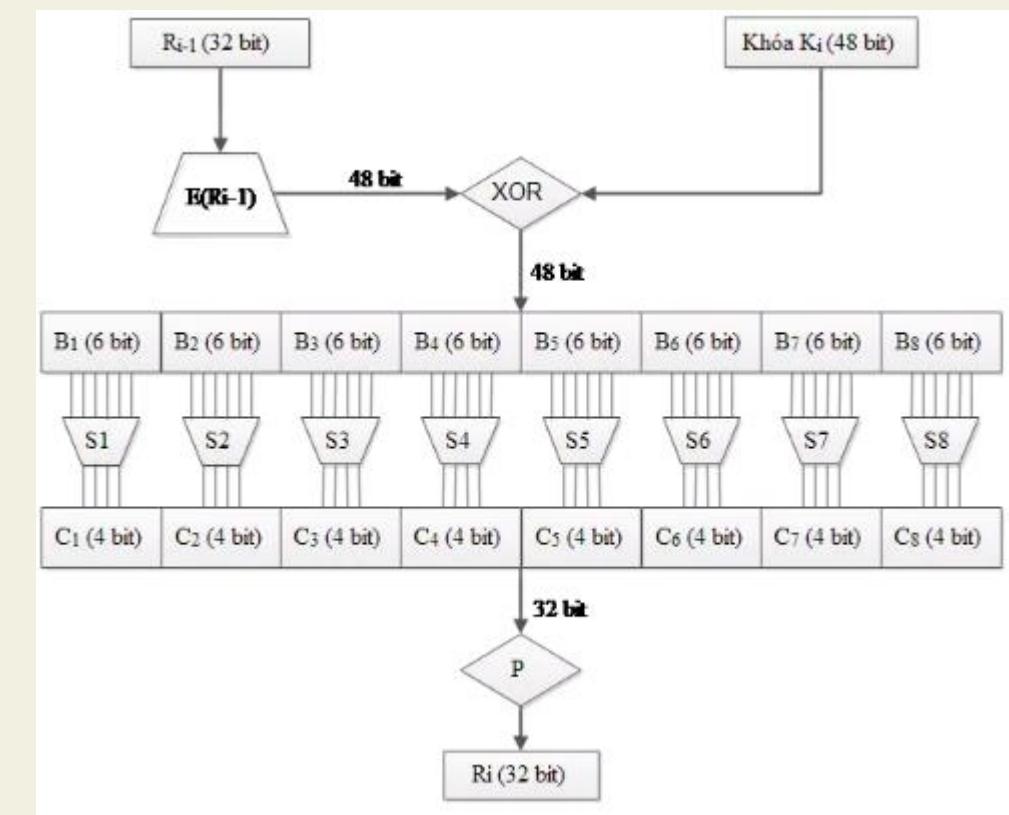
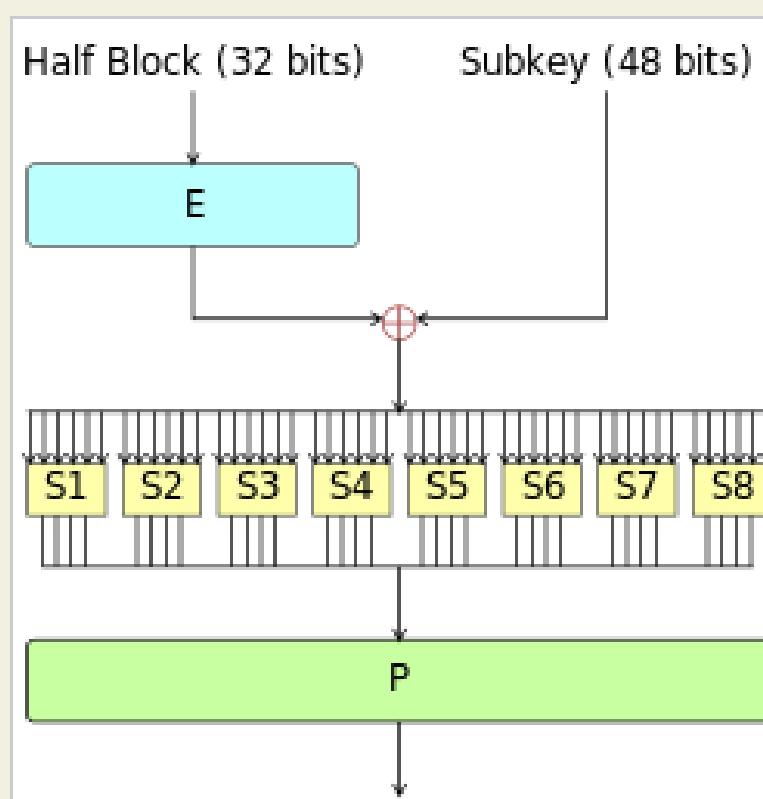
- IP là một phép hoán vị vị trí của các ký tự trong mỗi từ 64 bít, từ vị trí thứ nhất đến vị trí thứ 64.
- Bảng dưới đây cho ta phép hoán vị IP, với cách biểu diễn là bít thứ nhất của $IP(x)$ là bít thứ 58 của từ x (có 64 bít), bít thứ hai của $IP(x)$ là bít thứ 50 của x ,...
- Bảng của phép hoán vị IP^{-1} cũng được hiểu tương tự

IP									IP ⁻¹								
58	50	42	34	26	18	10	2		40	8	48	16	56	24	64	32	
60	52	44	36	28	20	12	4		39	7	47	15	55	23	63	31	
62	54	46	38	30	22	14	6		38	6	46	14	54	22	62	30	
64	56	48	40	32	24	16	8		37	5	45	13	53	21	61	29	
57	49	41	33	25	17	9	1		36	4	44	12	52	20	60	28	
59	51	43	35	27	19	11	3		35	3	43	11	51	19	59	27	
61	53	45	37	29	21	13	5		34	2	42	10	50	18	58	26	
63	55	47	39	31	23	15	7		33	1	41	9	49	17	57	25	

II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

- Sơ đồ hàm f (Feistel function):
- Hàm f lấy đầu vào là hai từ: R có 32 bít và K có 48 bít và có kết quả ở đầu ra là từ f(R,K) có 32 bít, được xác định bởi sơ đồ sau:



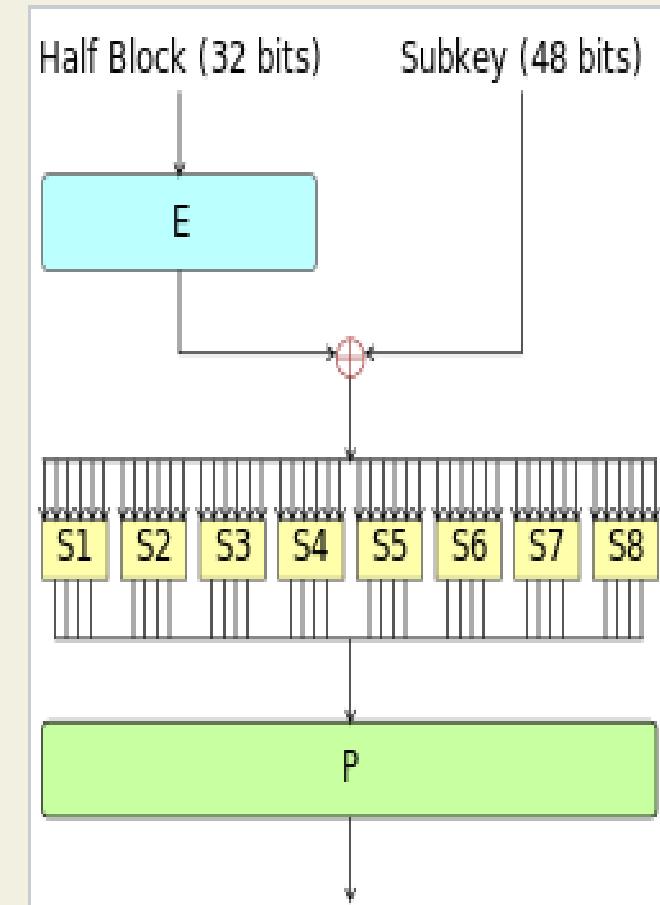
II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

- **Hàm E (Extension):** Là một phép hoán vị “mở rộng” theo nghĩa là nó biến mỗi từ R 32 bit thành từ E(R) bằng các hoán vị 32 bit của R nhưng có một số cặp bit được lặp lại để E(R) thành một từ có 48 bit.
- Cụ thể phép hoán vị “mở rộng” đó được cho bởi bảng sau:

Phép hoán vị “mở rộng” E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

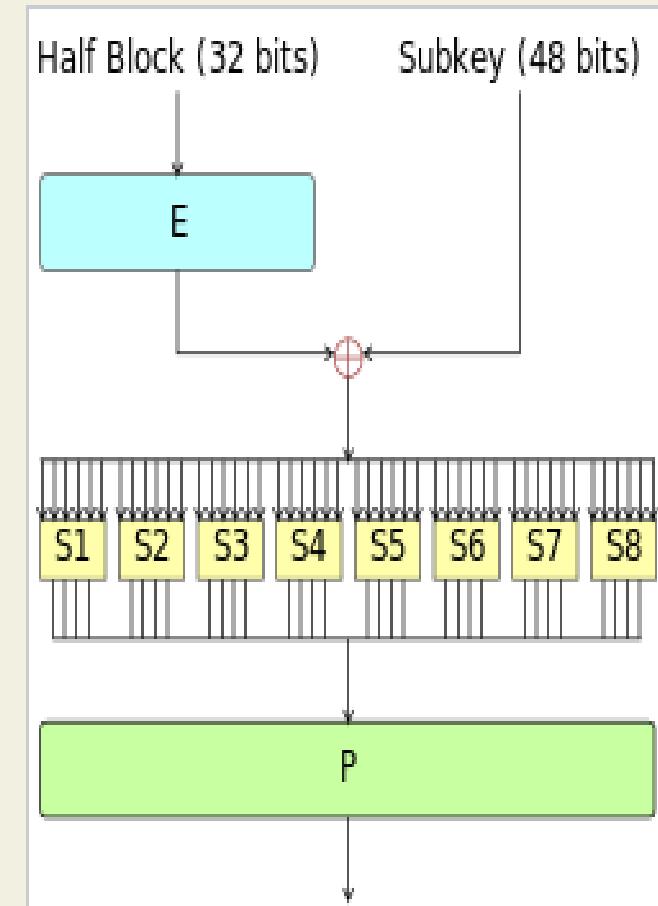
- Như vậy mỗi từ R= $a_1a_2\dots a_{32}$ sẽ biến thành $E(R)=a_{32}a_1a_2a_3a_4a_5a_4a_5\dots a_{30}a_{31}a_{32}a_1$



II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

- Sau khi thực hiện E, $E(R)$ sẽ được cộng (từng bít theo mod2) với K, được một từ 48 bít, chia thành 8 khối (6 bít)
- Mỗi hộp S_i ($i=1,..8$) là một phép thay thế, biến mỗi từ B_j 6 bít thành một từ C_j 4 bít; các hộp S_i được cho bởi bảng dưới đây với cách biểu diễn như sau:
- Cụ thể phép hoán vị “mở rộng” đó được cho bởi bảng sau:
- Mỗi từ $B_j=b_1b_2b_3b_4b_5b_6$ ứng với một vị trí (r,s) ở hàng thứ r và cột thứ s trong bảng, các hàng được đánh số thứ tự từ 0 đến 3 với biểu diễn nhị phân b_1b_6 và các cột được đánh số thứ tự từ 0 đến thứ 15 ứng với biểu diễn nhị phân $b_2b_3b_4b_5$.
- Nghĩa là $r=b_1b_6$; $s=b_2b_3b_4b_5$ (từ nhị phân chuyển sang thập phân)



II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

Ví dụ:

$$S_1(101110) = 11_d = 1011_b \text{ (hàng } r=10_b+1=3, \text{ cột } s=0111_b+1 = 8)$$

$$S_2(011000) = 12_d = 1100_b \text{ (hàng } r=00_b+1=1, \text{ cột } s=1100_b+1 = 13)$$

$$S_3(100110) = ?$$

S là bí mật
rất quan
trọng trong
bảo đảm
tính bí mật
của DES

S5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	0	14	2	13	6	15	0	9	10	4	5	3

S6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15				
0	4	11	2	S8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	13	0	11	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
2	1	4	11	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
3	6	11	13	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
				3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	3	0	6	9	10	1	2	8	5	11	12	4	15		
1	11	5	6	15	0	3	4	7	2	12	1	10	14	9		
2	9	0	12	11	7	13	15	1	3	14	5	2	8	4		
3	0	6	10	1	13	8	9	4	5	11	12	7	2	14		

Anh

II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

Phép hoán vị P trong sơ đồ của hàm f được cho ở bảng dưới đây:

Mỗi 4 bít đầu ra của các hộp S-box sẽ được ghép lại, theo thứ tự các hộp và được đưa vào hộp P-box. P đơn giản chỉ là phép hoán vị các bít với nhau.

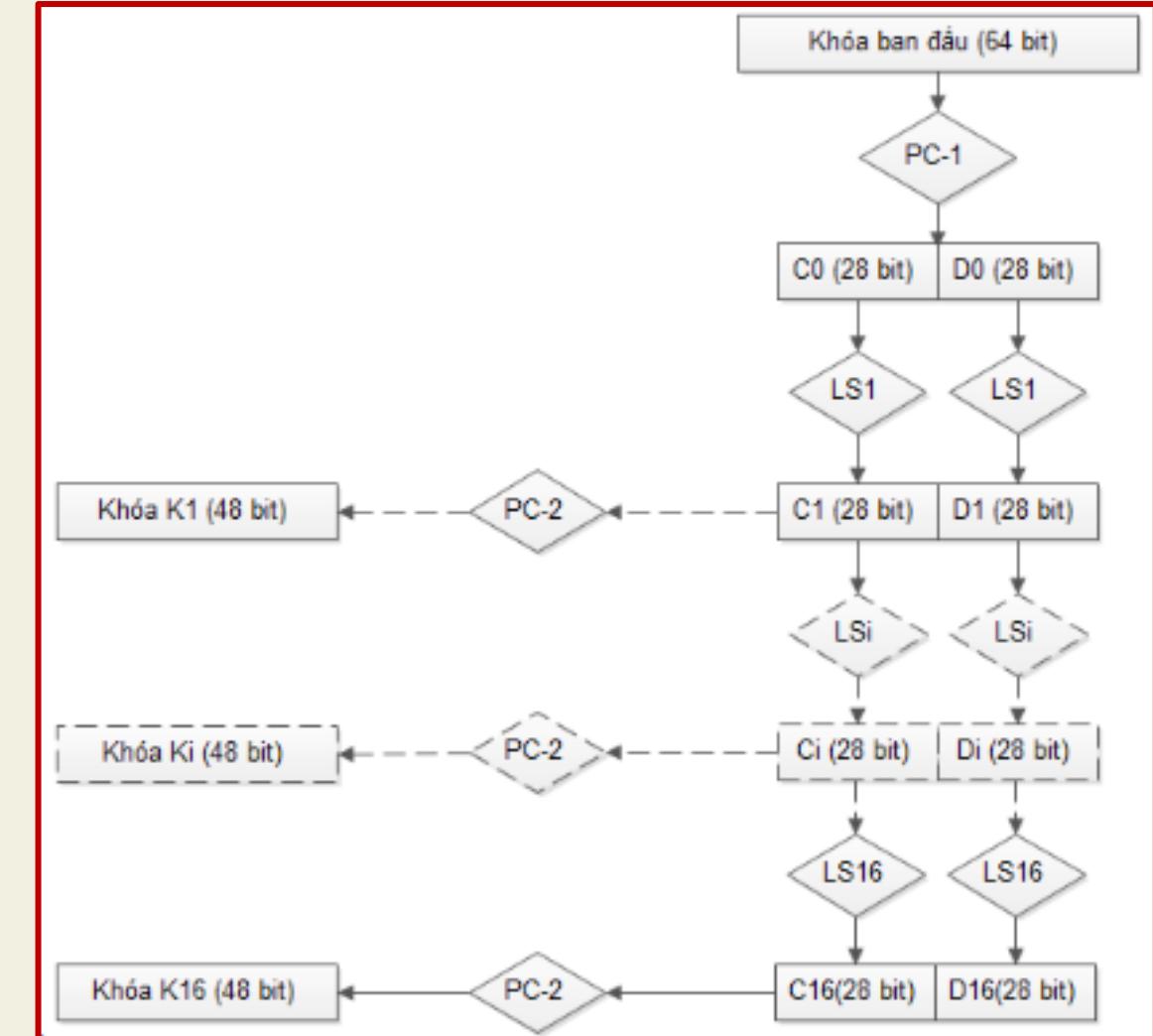
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Như vậy hàm f được xác định hoàn toàn

II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

- Thuật toán sinh khóa K_i : K_1, K_2, \dots, K_{16}
- Các khóa con đều được sinh ra từ khóa chính của DES bằng thuật toán sinh khóa con (thuật toán G)
- LS: left shift
- Khóa mật mã K là một từ 56 bit, ta chia thành 8 khối, mỗi khối 7 bit, ta cho thêm mỗi khối 7 bit đó một bit kiểm tra tính chẵn lẻ vào vị trí cuối để được một từ 64 bit, ta vẫn ký hiệu là K.



II. Mã hóa bí mật

2.3. Mật mã DES (Data Encryption Standard)

- Trước tiên, thuật toán PC-1 biến K thành một từ 56 bít, ta chia thành 2 nửa C0, D0.
- Phép hoán vị PC-1 được xác định bởi bảng sau đây

57	49	41	33	25	17	9	1
58	50	42	34	25	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

Chú ý: trong bảng không có các số 8,16,24,32,40,48,56,64 là vị trí của những bít được thêm vào khi hình thành từ mới K

II. Mã hóa bí mật

2.1. Mật mã DES (Data Encryption Standard)

- $Ls_i, i=1,2,\dots,16$ là phép chuyển dịch vòng sang trái:
VD: 00000100 dịch trái 2 bít thành 00010000
- Chuyển dịch một vị trí nếu $i=1,2,9,16$
- Chuyển dịch hai vị trí với giá trị i còn lại

Vòng lặp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Số lần dịch trái	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

- Phép hoán vị PC2 biến mỗi từ 56 bít CiDi thành từ 48 bít Ki theo bảng dưới đây

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

II. Mã hóa bí mật

Kết luận DES:

- Thuật toán mã hóa E:
 - $y = E(K, x)$ với mỗi khóa $K(K_1, K_2, \dots, K_{16})$ với bản rõ x
- Thuật toán giải mã D:
 - $x = D(K, y)$ được thực hiện bằng cùng một quá trình tính toán như quá trình mã hóa, chỉ khác là thứ tự dùng khóa K sẽ là $K_{16}, K_{15}, \dots, K_2, K_1$.
- Độ an toàn DES: 30 năm đầu sau khi công bố → khá an toàn
 - Với tốc độ xử lý của siêu máy tính thì với độ dài khóa chỉ 56 bit → tính an toàn bị phá vỡ

Table 2.2 Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55} \text{ ns} = 1.125 \text{ years}$	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127} \text{ ns} = 5.3 \times 10^{21} \text{ years}$	$5.3 \times 10^{17} \text{ years}$
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167} \text{ ns} = 5.8 \times 10^{33} \text{ years}$	$5.8 \times 10^{29} \text{ years}$
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191} \text{ ns} = 9.8 \times 10^{40} \text{ years}$	$9.8 \times 10^{36} \text{ years}$
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255} \text{ ns} = 1.8 \times 10^{60} \text{ years}$	$1.8 \times 10^{56} \text{ years}$

2.1 Mật mã DES (Data Encryption Standard)

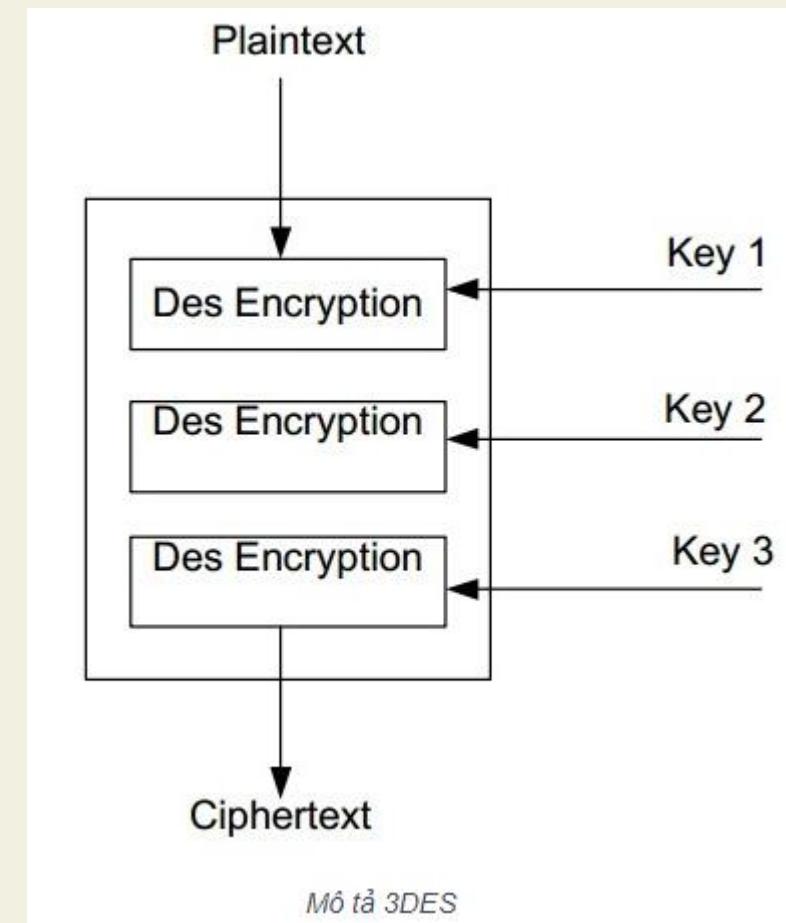
- **Bài tập áp dụng:**

- Cho bản rõ mang nội dung: $x = '0123456789ABCDEF'$; khóa $K = 13345799BBCDDFF1$
- Trong hệ cơ số 16, thực hiện mã hóa văn bản rõ trên theo thuật toán DES

II. Mã hóa bí mật

2.2. Mật mã 3-DES (Triple DES)

- Thuật toán mã hóa 3DES gồm 3 chìa khoá 64 bit, tức là toàn bộ chiều dài khoá là 192 bit: 03 khoá DES là K_1 , K_2 và K_3 .
- Thủ tục mã hóa cũng tương tự DES nhưng nó được lặp lại 3 lần tức là tăng lên 3 lần DES. Dữ liệu được mã hóa với chìa khoá đầu tiên, và được giải mã với chìa khoá 2, sau đó mã hóa lần nữa với chìa khoá thứ 3 để thu được dữ liệu mã hóa cuối cùng.
- Các mẫu hoạt động của 3DES:
 - Triple ECB (Triple Electronic Code Book): Sách mã hóa điện tử.
 - Triple CBC (Triple Cipher Chaining): Móc nối khối ký số.



2.2. Mật mã 3-DES (Triple DES)

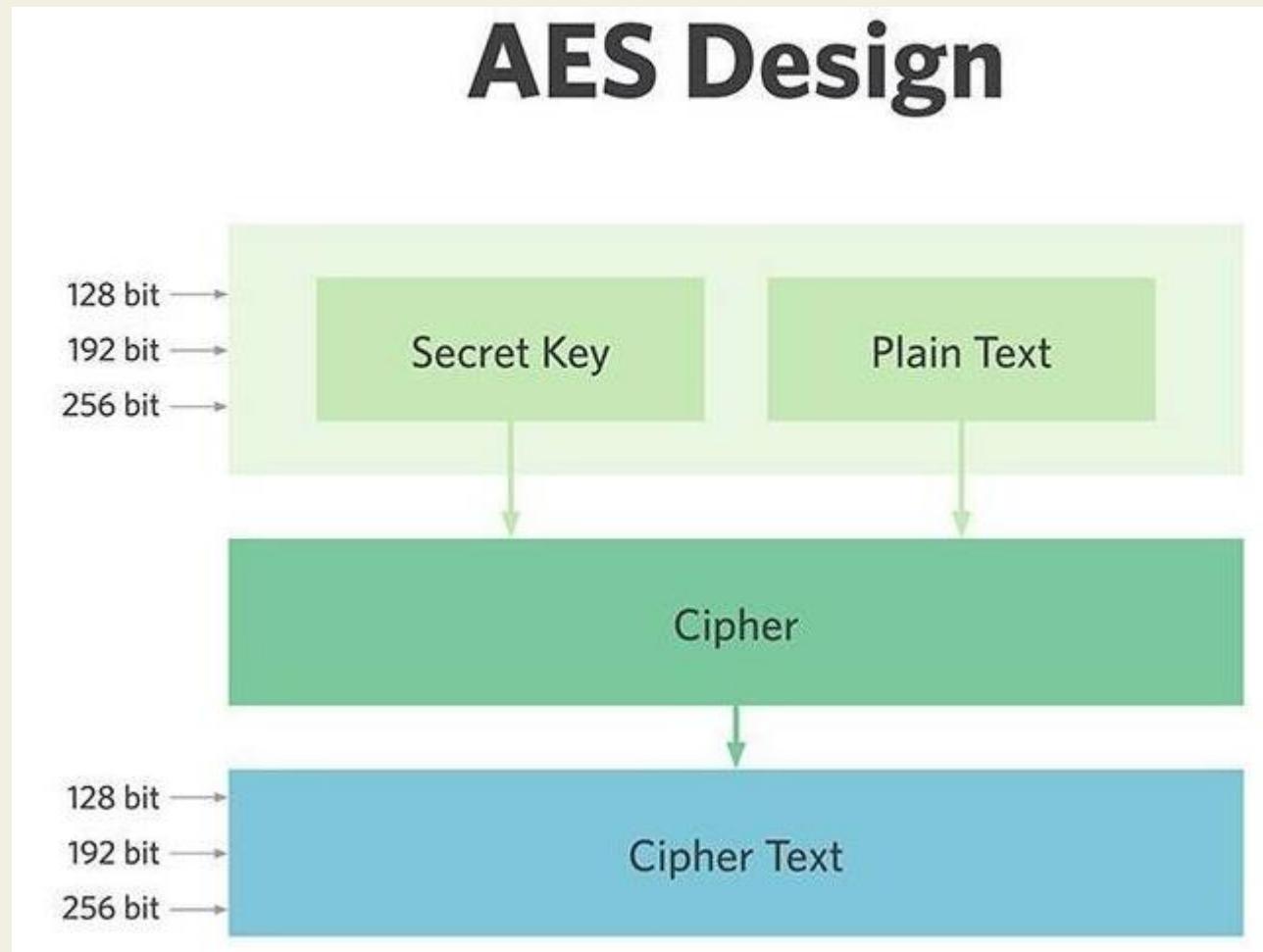
- **Ưu và nhược điểm của 3DES**

- **Ưu điểm:** Khác với DES, thuật toán mã hóa 3DES được mã hóa 3 lần DES với kích cỡ không gian khoá 168 bit cho nên an toàn hơn rất nhiều so với DES.
- **Nhược điểm:** Vì 3DES sử dụng 3 lần mã hóa DES cho nên tốc độ mã hóa sẽ chậm hơn rất nhiều so với DES. Phần mềm ứng dụng tỏ ra rất chậm đối với hình ảnh số và một số ứng dụng dữ liệu tốc độ cao vì kích thước khối 64 bit vẫn còn là một nhược điểm đối với những hệ thống hiện nay.

2.3. Mật mã AES (Advanced Encryption Standard)

- Được công bố lần đầu năm 1997 bởi NIST
- AES được nghiên cứu và phát triển để thay thế cho DES
- NIST tuyên bố AES là giải pháp tốt nhất để bảo vệ thông tin nhạy cảm cho chính phủ (Mỹ) trong thế kỷ 21
- AES gồm ba mật mã khối AES-128, AES-192, AES-256 tương ứng với độ dài của key là 128 bit, 192 bit và 256 bit. Số vòng của key khác nhau, cụ thể 10 vòng cho 128 bit, 12 vòng cho 192 bit và 14 vòng cho 256 bit.
- Mỗi vòng đều thực hiện ba bước thay thế, biến đổi và hòa trộn khối plain text (văn bản thuần túy) đầu vào để biến nó thành Ciphertext (văn bản đã mã hóa).

2.3. Mật mã 3AES (Advanced Encryption Standard)



AES có an toàn không?

- ✓ AES nếu được triển khai đúng quy trình thì sẽ đảm bảo an toàn tuyệt đối.
- ✓ Thế nhưng một điều cần lưu ý đó là bất kỳ một hệ thống nào cũng có thể bị tấn công nếu hacker biết được key mã hóa.
- ✓ Do đó các key mã hóa AES phải được bảo vệ bằng nhiều cách khác nhau như dùng mật khẩu mạnh, xác thực, tường lửa hay phần mềm chống độc hại.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Giới thiệu chung

- Vào năm 1999, cục tiêu chuẩn quốc gia Hoa Kỳ (NIST) đã ban hành một phiên bản mới của tiêu chuẩn DES chỉ ra rằng DES chỉ nên được sử dụng cho các hệ thống cũ và 3-DES được sử dụng.
- 3-DES có **2 ưu điểm** đảm bảo cho việc sử dụng rộng rãi trong vài năm tới:
 - Đầu tiên, với độ dài khóa 168-bit, nó khắc phục được lỗ hổng đối với cuộc tấn công vét cạn của DES.
 - Thứ hai, thuật toán mã hóa cơ bản trong 3-DES cũng giống như trong DES. → có khả năng chống thám mã tốt.
- 3-DES có **2 nhược điểm:**
 - Hạn chế chính của 3-DES là thuật toán tương đối chậm trong phần mềm. DES ban đầu được thiết kế để triển khai bằng phần cứng giữa những năm 1970 và không tạo ra mã phần mềm hiệu quả.
 - Một nhược điểm phụ là cả DES và 3-DES đều sử dụng kích thước khối 64-bit. Vì lý do cả hiệu quả và bảo mật, kích thước khối lớn hơn là cần thiết.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

- Để thay thế, vào năm 1997 NIST đã đưa ra lời kêu gọi đề xuất **Tiêu chuẩn mã hóa nâng cao (AES)** mới, tiêu chuẩn này phải có sức mạnh bảo mật bằng hoặc tốt hơn 3-DES và cải thiện đáng kể hiệu quả.
- NIST quy định rằng AES phải là mật mã khối đối xứng với độ dài khối 128 bit và hỗ trợ độ dài khóa có thể là 128, 192 và 256 bit
- NIST đã chọn Rijndael làm thuật toán AES được đề xuất. Hai nhà nghiên cứu đã phát triển và gửi Rijndael cho AES đều là những nhà mật mã học đến từ Bỉ: Tiến sĩ Joan Daemen và Tiến sĩ Vincent Rijmen.
- Cuối cùng, AES được thiết kế để thay thế 3-DES, nhưng quá trình này sẽ mất một số năm. NIST dự đoán rằng DES ba lần vẫn sẽ là một thuật toán được sử dụng trong tương lai gần.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

- Bảng dưới liệt kê tham số của AES tùy thuộc vào kích thước của khóa. Trong phần này ta lựa chọn khóa 128 bits là kích thước thông dụng thường được triển khai trong thực tế

Kích thước khóa (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Kích thước khối của bản rõ (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Số vòng	10	12	14
Kích thước khóa tại mỗi vòng (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Kích thước khóa mở rộng (words/bytes)	44/176	52/208	60/240

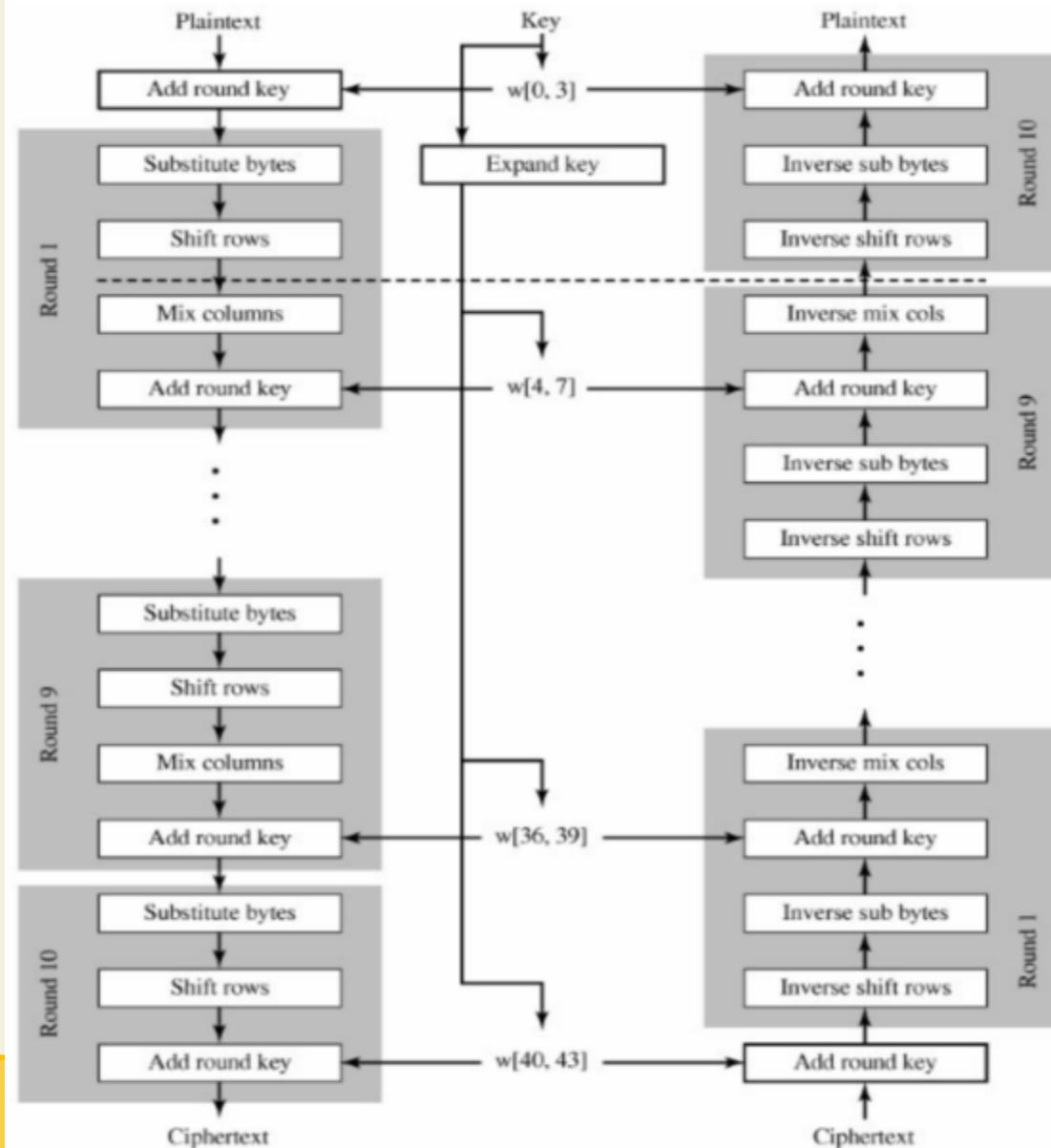
Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

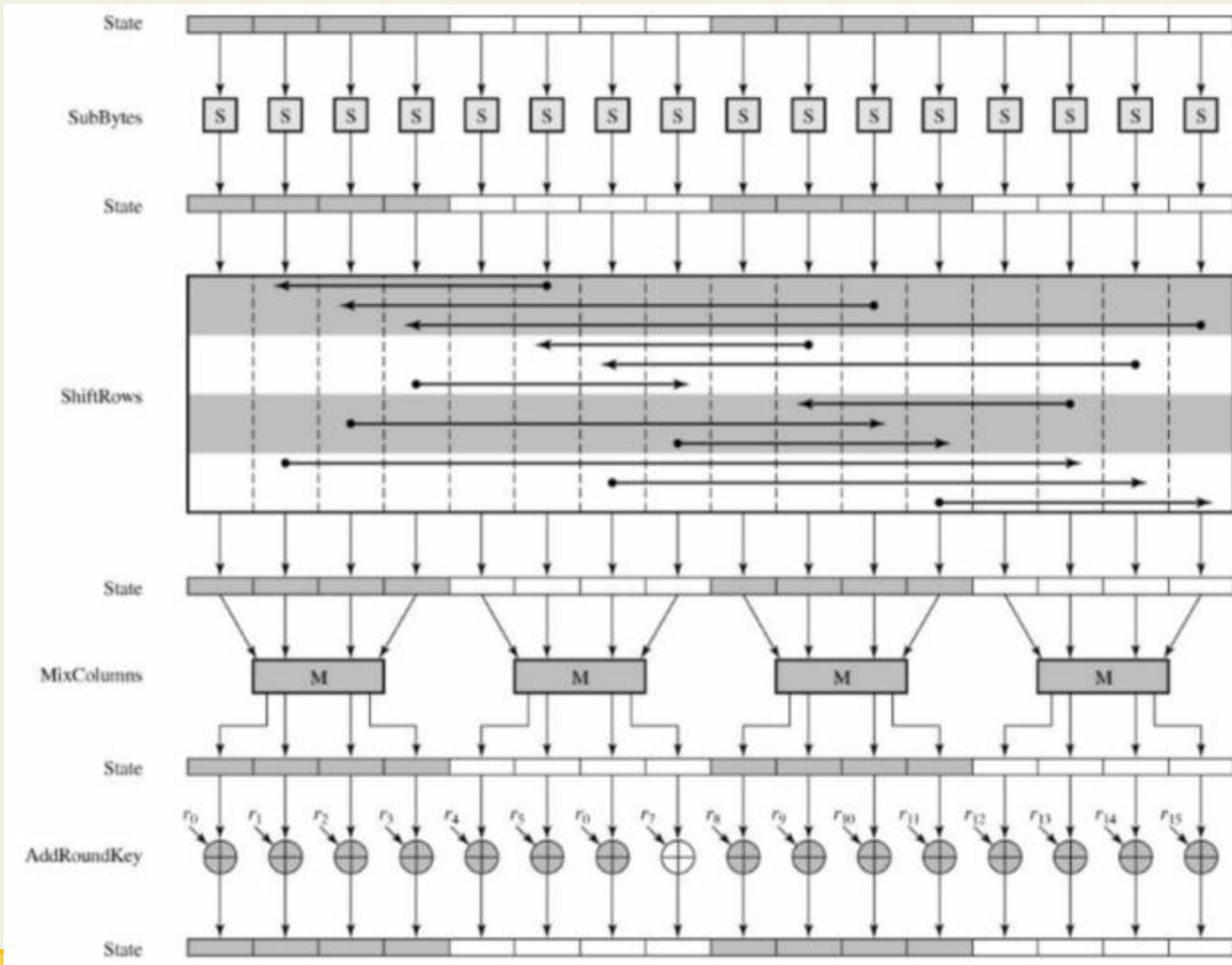
- Đầu vào cho thuật toán mã hóa và giải mã là một khối 128 bít, khối bít này được mô tả là một ma trận vuông, mỗi ô là 1 byte;
- Khối này được sao chép vào một mảng trạng thái, được sửa đổi ở mỗi giai đoạn mã hóa hoặc giải mã;
- Sau giai đoạn cuối cùng, mảng trạng thái này được sao chép vào một ma trận đầu ra.
- Tương tự, khóa 128 bit được mô tả như một ma trận vuông, mỗi phần tử là một byte;
- Khóa này sau đó được mở rộng thành một mảng các từ (word), mỗi từ là bốn byte và tổng chiều dài khóa là 44 từ cho khóa 128 bit
- Lưu ý rằng thứ tự của các byte trong ma trận là theo cột.
- Vì vậy, bốn byte đầu tiên của bản rõ 128 bit đầu vào chiếm cột đầu tiên của ma trận, bốn byte thứ hai chiếm cột thứ hai, v.v. Tương tự, bốn byte đầu tiên của khóa mở rộng, tạo thành một từ, chiếm cột đầu tiên của ma trận w.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Cấu trúc mã hóa và giải mã AES



Chuẩn mã nâng cao (AES – Advanced Encryption Standard)



Một vòng
mã hóa
đầy đủ
AES

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

Cả thuật toán mã hóa và giải mã đều bắt đầu giai đoạn AddRoundKey, tiếp theo là **9 vòng**, mỗi vòng đầy đủ **4 giai đoạn**:

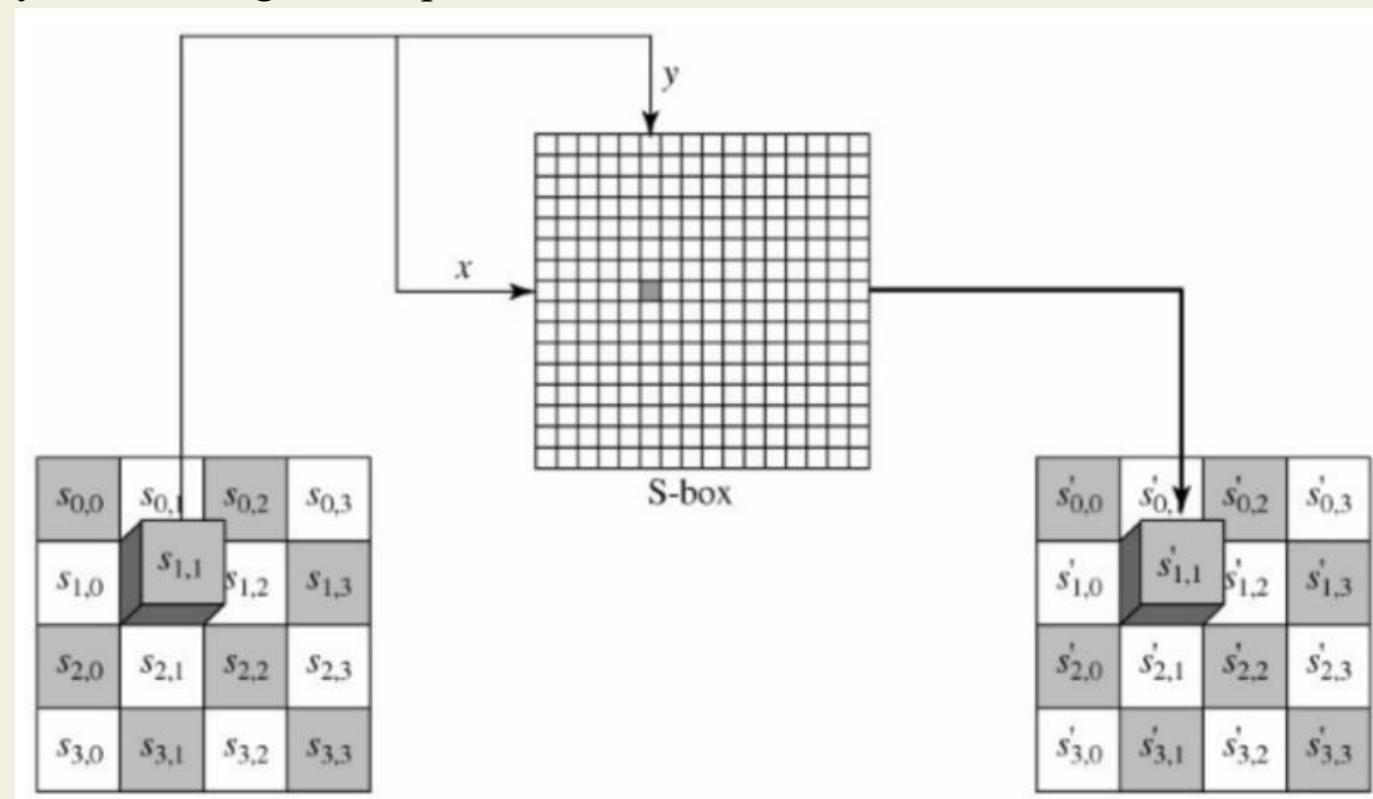
- ❖ Thay thế các bytes (*Substitute bytes*) sử dụng hộp S để thực hiện việc thay thế từng byte của khối;
- ❖ Dịch các dòng (*ShiftRows*) đơn giản là thực hiện hoán vị;
- ❖ Trộn cột (*MixColumns*) là phép thay thế sử dụng các phép toán số học trên Z_{256} ;
- ❖ *AddRoundKey* đơn giản chỉ là phép XOR của khối hiện tại với một phần của khóa được mở rộng.

Vòng cuối cùng chỉ có 3 giai đoạn.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

- **Hàm SubBytes:** Thay thế byte đơn giản chỉ là tra cứu trong bảng 16×16 , mỗi ô là 1 byte và được gọi là hộp S-box và S-box đảo.



Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

- Hàm SubBytes: S-box

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

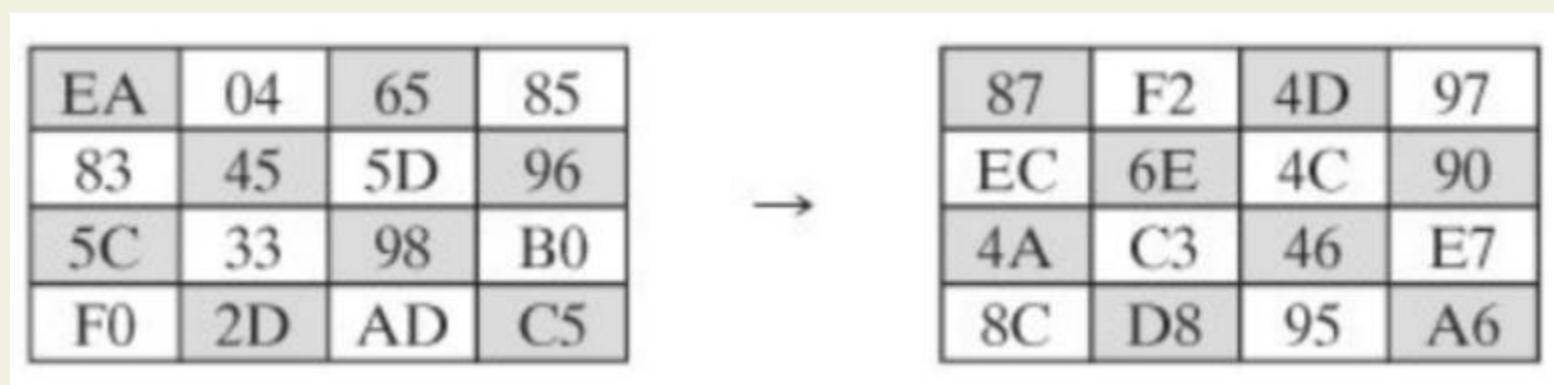
- **Hàm SubBytes:** *Hộp S đảo (inverse S box)*

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

- **Hàm SubBytes:** Ví dụ minh họa phép thay thế byte



EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

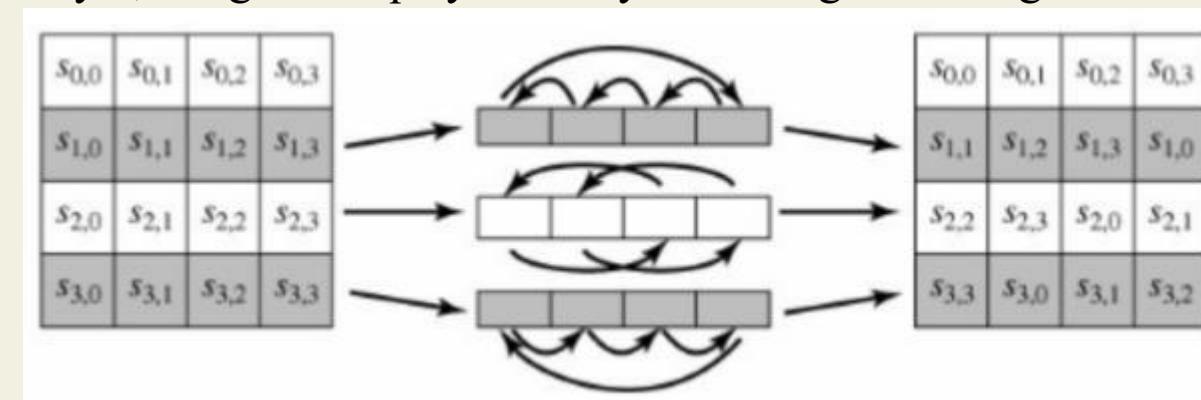
Tìm byte thay thế của EA: Tra dòng E và cột A trong S-box được 87. Vậy thay thế EA bằng 87

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

Dịch dòng (Shiftrows): Dòng đầu tiên của ma trận trạng thái được giữ nguyên, dòng thứ hai quay trái 1 byte, dòng thứ 3 quay trái 2 byte và dòng cuối cùng quay trái 3 byte.

*Minh họa
phép dịch
dòng*



*Ví dụ minh họa
phép dịch dòng*

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

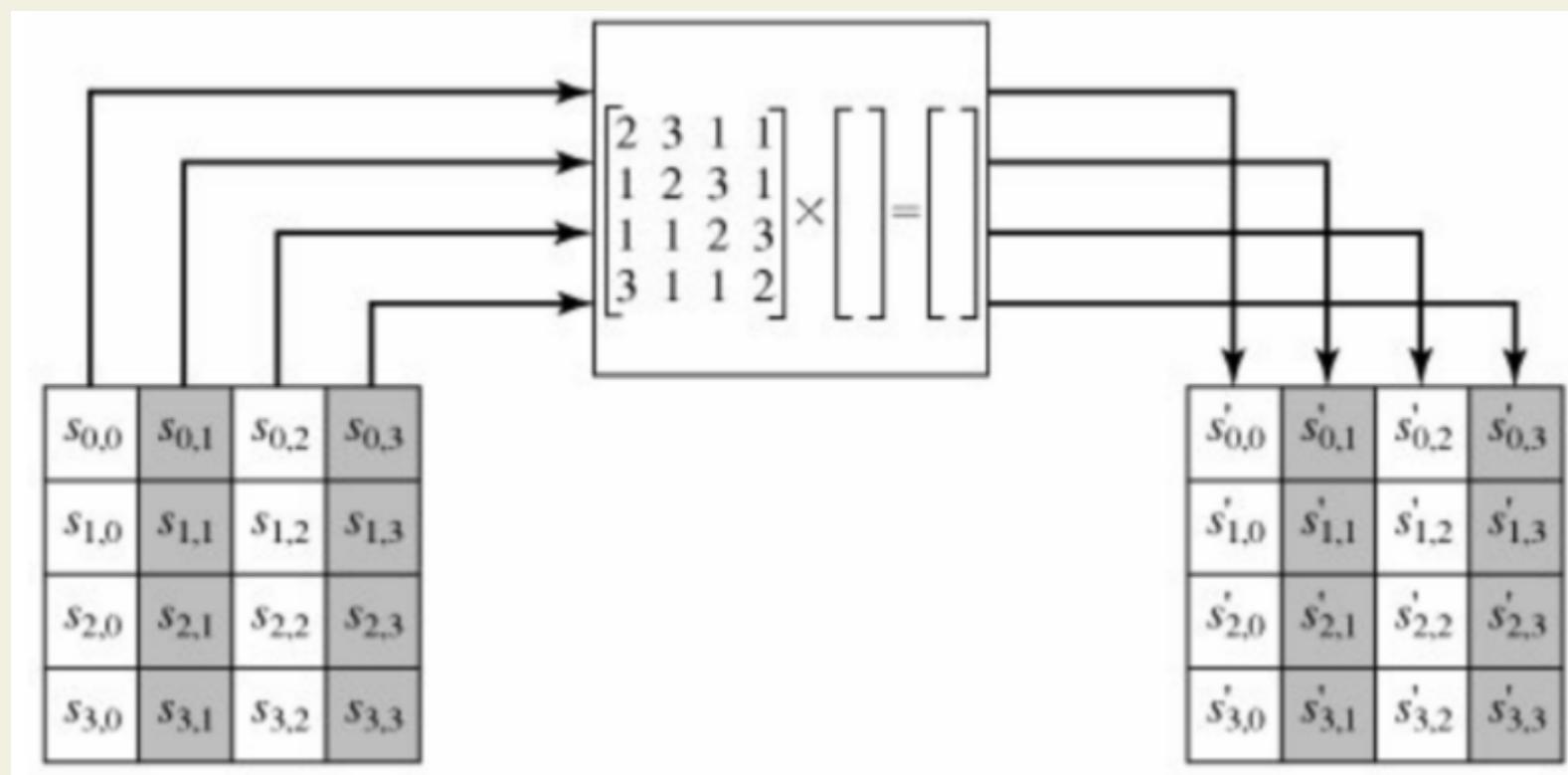
87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Đối với thuật toán giải mã ta sử dụng phép dịch dòng ngược.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

Trộn cột: Phép trộn cột được thực hiện như minh họa



Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

Trộn cột: Kết quả phép trộn cột được tính như sau:

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

Áp dụng phép nhân hai ma trận ta có?

$$s'_{0,j} = (2 \cdot s_{0,j}) + (3 \cdot s_{1,j}) + s_{2,j} + s_{3,j}$$

$$s'_{1,j} = s_{0,j} + (2 \cdot s_{1,j}) + (3 \cdot s_{2,j}) + s_{3,j}$$

$$s'_{2,j} = s_{0,j} + s_{1,j} + (2 \cdot s_{2,j}) + (3 \cdot s_{3,j})$$

$$s'_{3,j} = (3 \cdot s_{0,j}) + s_{1,j} + s_{2,j} + (2 \cdot s_{3,j})$$

Trong đó, phép nhân(.) được thực hiện theo luật sau: Giả sử $s_{i,j}$ được biểu diễn dưới dạng 8 bit $b_7b_6b_5b_4b_3b_2b_1b_0$ khi nhân với 2 sẽ được thực hiện theo công thức sau:

$$2 \cdot s_{i,j} = \begin{cases} b_6b_5b_4b_3b_2b_1b_0 & \text{nếu } b_7 = 0 \\ b_6b_5b_4b_3b_2b_1b_0 + 00011011 & \text{nếu } b_7 = 1 \end{cases}$$

$$3 \cdot s_{i,j} = s_{i,j} + 2 \cdot s_{i,j}$$

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

Trộn cột:

Ví dụ minh họa

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

→

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

Ta diễn giải cách xác định phần tử đầu tiên trong ma trận sau khi thực hiện phép trộn cột.

$$s'_{0,0} = 2 \cdot (87) + 3 \cdot (6E) + 46 + A6$$

Chuyển các số từ hệ 16 sang hệ 2 thu được $87h = 10000111$. Do bít $b_7 = 1$ nên
 $2.(87) = 00001110 XOR 00011011 = 00010101$, $6Eh = 01101110$, $46h = 01000110$,
 $A6h = 10100110$ và $3.(6E) = 6E + 2.(6E)$.
Do bít b_7 của $6E$ là 0 nên $2.(6E) = 11011100$.
Do đó, $3.(6E) = 01101110 XOR 11011100 = 10110010$.

2.(87)	=	0	0	0	1	0	1	0	1	
3.(6E)	=	1	0	1	1	0	0	1	0	
46	=	0	1	0	0	0	1	1	0	
A6	=	1	0	1	0	0	1	1	0	
XOR		0	1	0	0	0	1	1	1	
		$= 47h$								

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Giải mã AES ??

Trộn cột: Phép chuyển đổi đảo trộn cột (inverse mix column transform) trong thuật toán giải mã được thực hiện như sau:

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

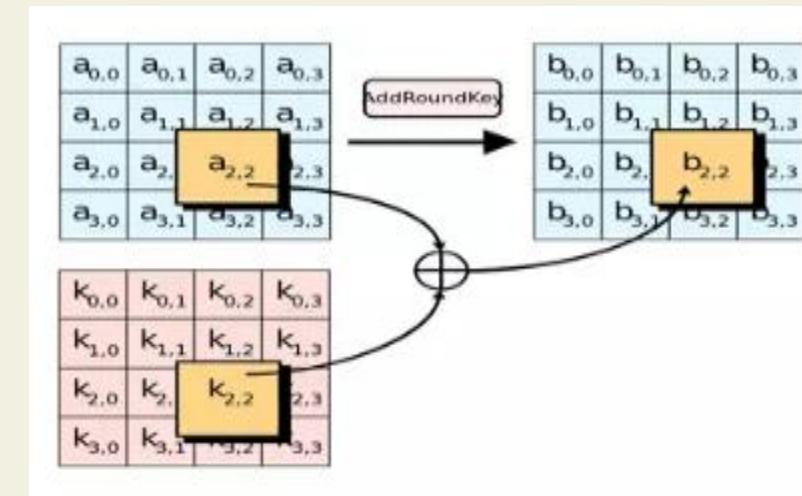
Thay thế công thức của phép trộn cột vào thì ta thu được công thức sau.

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán Mã hóa AES:

- Hàm AddRoundKey:** phép cộng với khóa là thực hiện phép XOR bít của 128 bít của ma trận trạng thái và 128 bít của khóa tương ứng của vòng. Mỗi khóa vòng gồm có 4 từ (128 bit) được lấy từ lịch trình khóa. 4 từ đó được cộng vào mỗi cột của state, sao cho:



<table border="1"> <tr><td>47</td><td>40</td><td>A3</td><td>4C</td></tr> <tr><td>37</td><td>D4</td><td>70</td><td>9F</td></tr> <tr><td>94</td><td>E4</td><td>3A</td><td>42</td></tr> <tr><td>ED</td><td>A5</td><td>A6</td><td>BC</td></tr> </table>	47	40	A3	4C	37	D4	70	9F	94	E4	3A	42	ED	A5	A6	BC	\oplus	<table border="1"> <tr><td>AC</td><td>19</td><td>28</td><td>57</td></tr> <tr><td>77</td><td>FA</td><td>D1</td><td>5C</td></tr> <tr><td>66</td><td>DC</td><td>29</td><td>00</td></tr> <tr><td>F3</td><td>21</td><td>41</td><td>6A</td></tr> </table>	AC	19	28	57	77	FA	D1	5C	66	DC	29	00	F3	21	41	6A	=	<table border="1"> <tr><td>EB</td><td>59</td><td>8B</td><td>1B</td></tr> <tr><td>40</td><td>2E</td><td>A1</td><td>C3</td></tr> <tr><td>F2</td><td>38</td><td>13</td><td>42</td></tr> <tr><td>1E</td><td>84</td><td>E7</td><td>D2</td></tr> </table>	EB	59	8B	1B	40	2E	A1	C3	F2	38	13	42	1E	84	E7	D2
47	40	A3	4C																																																	
37	D4	70	9F																																																	
94	E4	3A	42																																																	
ED	A5	A6	BC																																																	
AC	19	28	57																																																	
77	FA	D1	5C																																																	
66	DC	29	00																																																	
F3	21	41	6A																																																	
EB	59	8B	1B																																																	
40	2E	A1	C3																																																	
F2	38	13	42																																																	
1E	84	E7	D2																																																	

Ví dụ minh họa: Phép cộng khóa

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

- *Mở rộng khóa*

Thuật toán mở rộng khóa có đầu vào là 4 từ (16 bytes) khóa và tạo ra một mảng đầu ra 44 từ (176 bytes). Mã giả của thuật toán được mô tả như sau:

```
KeyExpansion (byte key[16], word w[44])  
{  
    word temp  
    for(i=0;i<4;i++)  
        w[i] = (key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])  
    for(i=4, i<44; i++)  
    {  
        temp = w[i-1]  
        if(i mod 4 = 0)  
            temp = SubWord(RotWord(temp)) XOR Rcon[i/4]  
        w[i] = w[i-4] XOR temp  
    }  
}
```

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

- *Mở rộng khóa*

Trong đó, phép toán **RotWord** là thực hiện phép quay trái 1 byte, tức là đầu vào 1 từ có 4 byte $[b_0, b_1, b_2, b_3]$ thì kết quả sau khi thực hiện phép quay trái 1 byte sẽ là $[b_1, b_2, b_3, b_0]$.

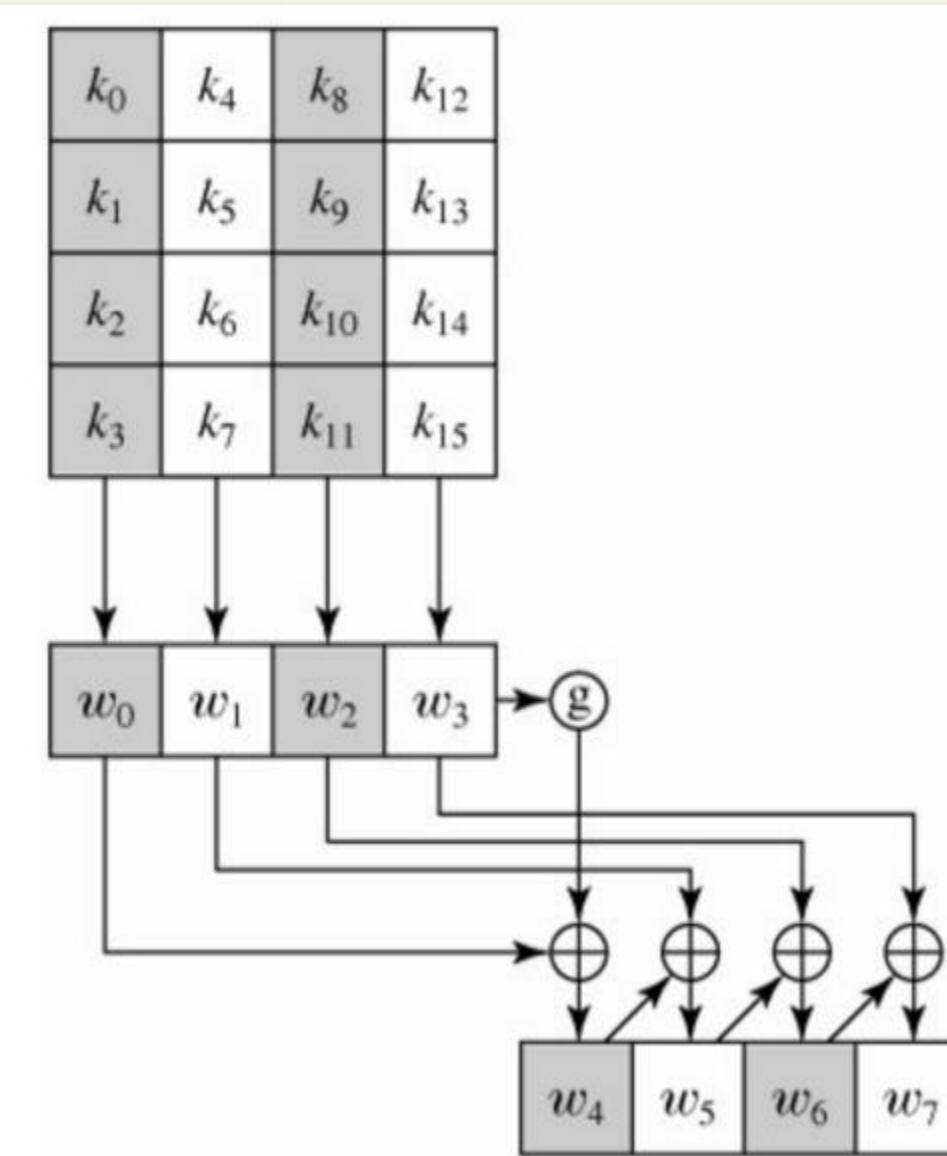
Phép toán **SubWord** là phép thay thế byte sử dụng bảng S. Hằng số cho mỗi vòng khóa $Rcon[j] = (RC[j], 0, 0, 0)$, với $RC[1] = 1$, $RC[j] = 2 \cdot RC[j-1]$ và phép nhân (\cdot) được thực hiện theo luật như trong thuật toán trộn cột.

Giá trị của $RC[j]$ được xác định như bảng dưới ở hệ thập lục phân (hexadecimal).

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

*Minh họa cách xác định
khóa của vòng 1*



Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

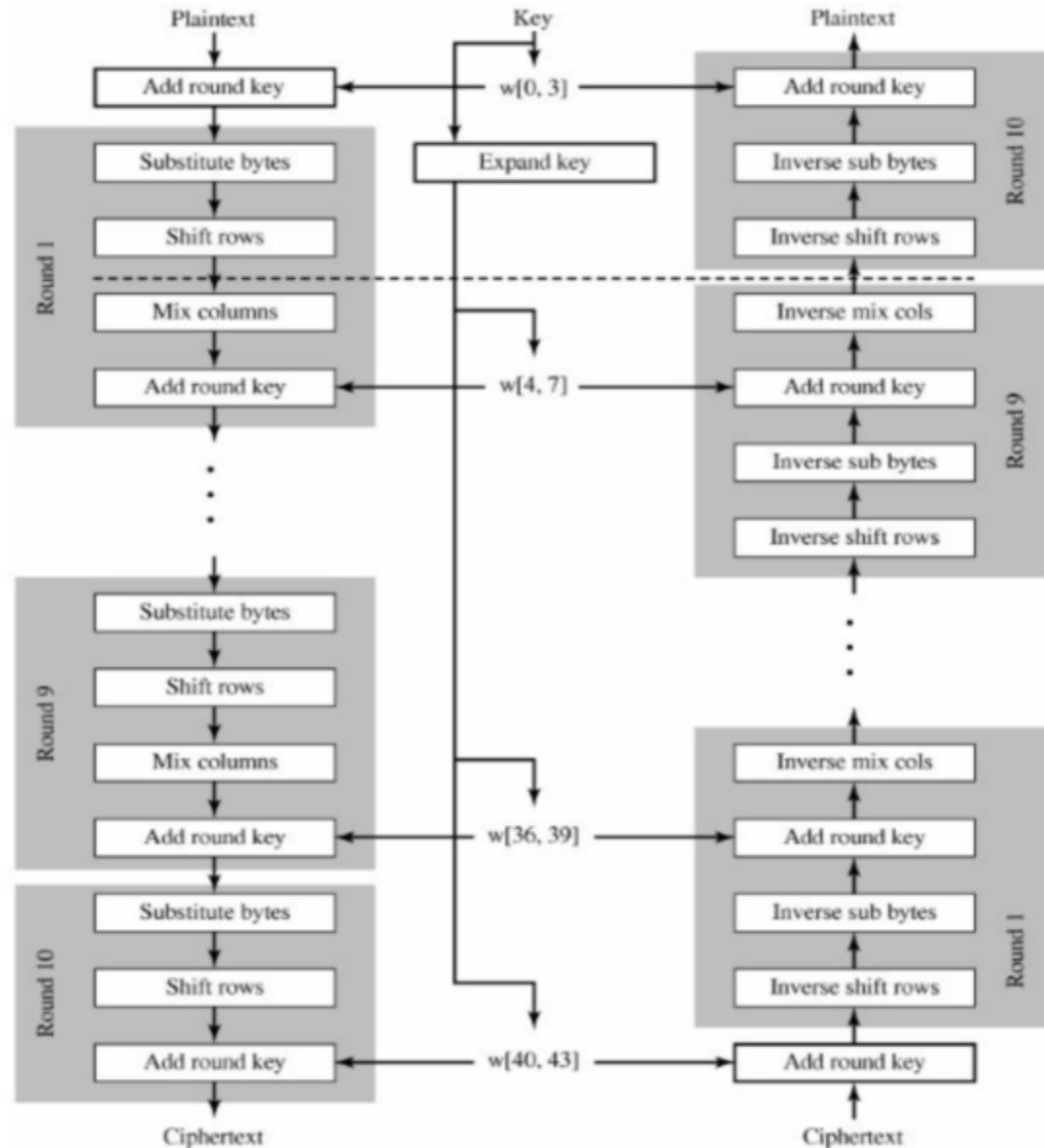
- Ví dụ minh họa cách xác định khóa cho vòng thứ 9 khi khóa tại vòng 8 là EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F tương ứng $w[32] = [EA, D2, 73, 21]$, $w[33] = [B5, 8D, BA, D2]$, $w[34] = [31, 2B, F5, 60]$ và $w[35] = [7F, 8D, 29, 2F]$. Giá trị của khóa tại vòng 9 được xác định như bảng sau:

Ví dụ xác định khóa tại vòng 8

Giá trị i ở hệ thập phân	temp	Sau khi thực hiện phép RotWord	Sau khi thực hiện phép SubWord	Rcon(9)	Sau khi XOR với Rcon	w[i-4]	w[i] = temp XOR w[i-4]
36	7F8D292F	8D292F7F	5DA515D2	1B000000	46A515D2	EAD27321	AC7766F3
37	AC7766F3	AC7766F3	AC7766F3	1B000000	AC7766F3	B58DBAD2	19FABC21
38	19FABC21	19FABC21	19FABC21	1B000000	19FABC21	312BF560	28B14941
39	28B14941	28B14941	28B14941	1B000000	28B14941	7F8D292F	575C606E

Như vậy, khóa của vòng 9 sẽ là AC 77 66 F3 19 FA BC 21 28 B1 49 41 57 5C 60 6E.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)



- **Thuật toán giải mã:** ngược lại với mã hóa

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Thuật toán giải mã:

- Thuật toán giải mã khá giống với thuật toán mã hóa về mặt cấu trúc nhưng 4 hàm sử dụng là 4 hàm ngược của các bước của thuật toán mã hóa.

Mã Hóa	Giải Mã
AddRoundKey()	InvAddRoundKey()
SubBytes()	InvSubBytes()
ShiftRows()	InvShiftRows()
MixColumns()	InvMixColumns()

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Tấn công AES và phương pháp phòng chống

- ✓ ***Side-channel attack***: Tấn công kênh phụ (định nghĩa là các kênh đầu ra không mong muốn từ một hệ thống)

Tấn công kênh bên hay còn gọi là Tấn công kênh phụ là loại tấn công dễ thực hiện trong các loại tấn công mạnh chống lại quá trình triển khai mã hóa, và mục tiêu của loại tấn công này là phân tích các nguyên tố, các giao thức, modul, và các thiết bị trong mỗi hệ thống.

- ✓ ***Known attacks***: Vào năm 2002, Nicolas Courtois và Josef Pieprzyk phát hiện một tấn công trên lý thuyết gọi là tấn công XSL và chỉ ra điểm yếu tiềm tàng của AES.

Tuy nhiên, một vài chuyên gia về mật mã học khác cũng chỉ ra một số vấn đề trong cơ sở toán học của tấn công này và cho rằng các tác giả đã có sai lầm trong tính toán. Việc tấn công dạng này có thực sự trở thành hiện thực hay không vẫn còn đe ngợ và cho tới nay thì tấn công XSL vẫn chỉ là suy đoán.

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

Phương pháp phòng chống tấn công AES:

- ✓ Sử dụng mã hóa mạnh: Sử dụng các biện pháp để tăng tính bảo mật của thuật toán mã hóa
- ✓ Bảo vệ dữ liệu theo phương pháp vật lý: chống lại tấn công side-channel attack
- ✓ Kết hợp cả hai phương pháp trên

Chuẩn mã nâng cao (AES – Advanced Encryption Standard)

KẾT LUẬN:

- **AES có an toàn không?** AES nếu được triển khai đúng quy trình thì sẽ đảm bảo an toàn tuyệt đối
- **Advanced Encryption Standard (AES)** là người bạn đồng hành không thể thiếu của chính phủ, cơ quan Nhà nước và tổ chức tư nhân.
- An toàn Thiết kế và độ dài khóa của thuật toán AES (128,192 và 256 bit) là đủ an toàn để bảo vệ các thông tin TỐI MẬT.Các thông tin TUYỆT MẬT phải dùng khóa 192 hoặc 256 bit.

BÀI TẬP ÔN TẬP

- **Bài 1:** Tìm kết quả phép thay thế byte của thuật toán AES cho ma trận trạng thái đầu vào sau:

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

- **Bài 2:** Tìm kết quả phép trộn cột của thuật toán AES cho ma trận trạng thái đầu vào sau:

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

- Vì sao lại ra đời mã hóa công khai?

+ Mã hóa bí mật – 1 khóa bí mật sử dụng cho cả mã hóa và giải mã

+ Khóa bí mật phải được chia sẻ trên kênh bí mật

+ Đảm bảo an toàn cho kênh bí mật có đơn giản?

→ Không cần trao đổi khóa

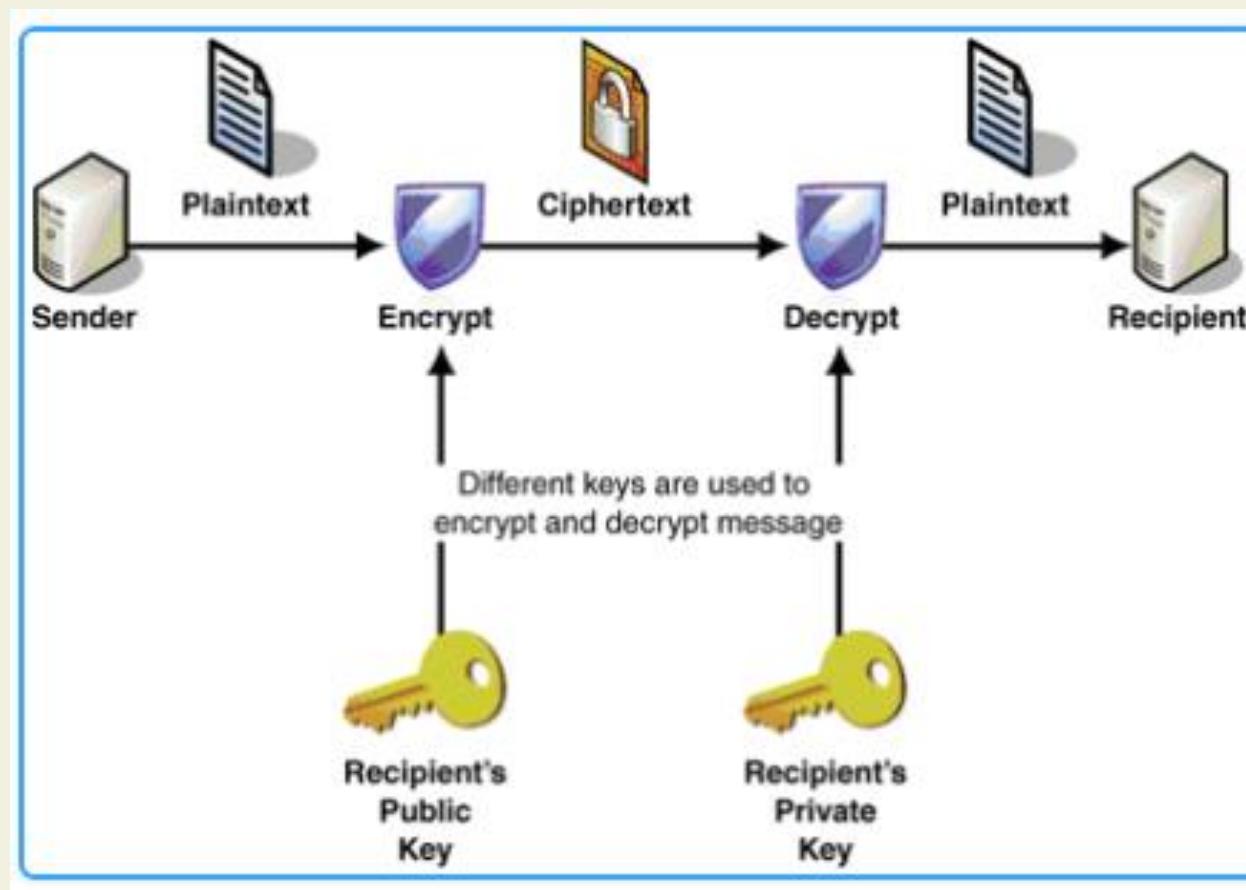
→ Mã hóa công khai ra đời



• Sự ra đời:

- Ý tưởng về mã hóa công khai được Diffie và Hellman đưa ra năm 1976
- Tuy nhiên, việc thực hiện hệ mật công khai thì do Rivest, Shamir và Adleman đưa ra đầu tiên năm 1977 → Mã hóa công khai RSA
- Sau đó là hệ mật ElGamal, hay dựa trên đường cong Elliptics ra đời
- Đặc điểm chung của các hệ mật này là xuất phát từ **toán học**

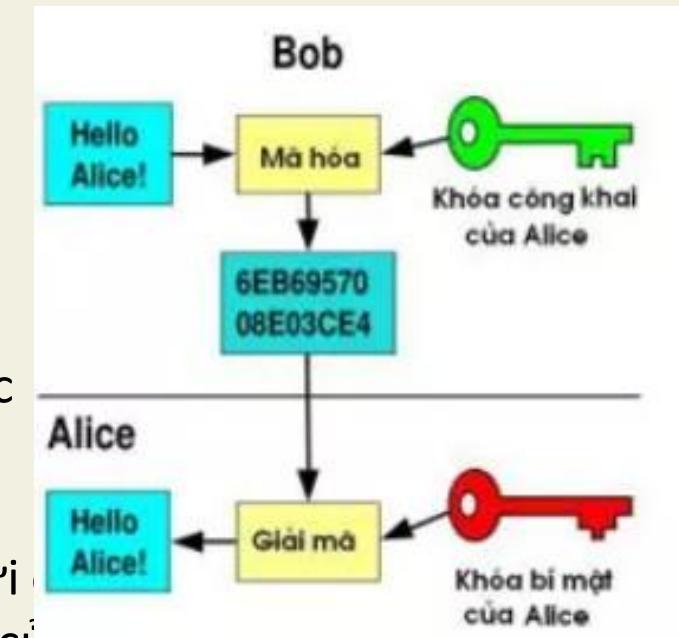
Sơ đồ tổng quát



III. Mã hóa công khai

Ý tưởng của mã hóa công khai

- ✓ Bob và Alice muốn gửi tin nhắn cho nhau
 - ✓ Alice sẽ tạo ra 2 khóa: 01 khóa công khai, 01 khóa bí mật
 - ✓ Trong đó:
 - Khóa công khai của Alice tất cả mọi người đều biết
 - Khóa bí mật chỉ 1 mình Alice biết
 - Khóa công khai và khóa bí mật liên hệ với nhau qua cơ chế toán học
 - Có khóa công khai cũng không suy ra được khóa bí mật
- Không cần chia sẻ khóa, Bob sẽ biết được khóa công khai của Alice
- ✓ **Bob** sẽ dùng **khóa công khai** của Alice để mã hóa bản tin mà Bob muốn gửi
 - ✓ Khi nhận được bản tin đã được mã hóa từ Bob, Alice sẽ dùng khóa bí mật của để giải mã bản tin
 - ✓ Tương tự với chiều gửi tin nhắn từ Alice tới Bob, Bob cũng biết khóa công khai của Alice, còn khóa bí mật của Bob thì chỉ 1 mình Bob biết



Với thuật toán mã hóa công khai chúng ta sẽ đi vào cơ
chế toán học sinh cặp khóa này.

Hệ mật RSA:

- Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT)
- Là hệ mật phù hợp nhất tạo ra chữ ký số điện tử đồng thời với việc mã hóa
- Đánh dấu sự tiến bộ vượt bậc của khoa học mật mã
- RSA được sử dụng phổ biến trong thương mại điện tử

Hệ mật RSA

Thuật toán sinh khóa trong RSA

Vấn đề cốt lõi của sinh khóa trong RSA là tìm được bộ 3 số tự nhiên e, d, và n sao cho:

$$m^{ed} \equiv m \pmod{n}$$

Ở đây: m – là số tự nhiên được chuyển hóa từ bản rõ M

(d,n) – là khóa bí mật

(e,n) – là khóa công khai

Cần phải bảo mật d sao cho dù biết e và n hay thậm chí cả “m” cũng không thể tìm ra được “d”

Hệ mật RSA

Bài toán RSA:

Cho một số nguyên dương: $n=p*q$

Trong đó p,q là hai thừa số nguyên tố (khác 2)

Một số nguyên dương b sao cho:

$\text{USCLN}(b, (p-1)(q-1))=1$

Và một số nguyên c

Bài toán đặt ra: Tìm số nguyên x sao cho

$$x^b \equiv c \pmod{n}$$

→ Giải được bài toán này là giải mã được

Hệ mật RSA

Thuật toán: Sinh khóa cho hệ mật RSA

1. Sinh hai số nguyên tố lớn p và q có giá trị xấp xỉ nhau

2. Tính $n=p \cdot q$, và $\phi(n) = (p-1)(q-1)$

3. Chọn một số ngẫu nhiên e , $1 < e < \phi(n)$

sao cho $\gcd(e, \phi(n)) = 1$

4. Sử dụng thuật toán Euclide mở rộng để tính số d , $1 < d < \phi(n)$

Sao cho $e \cdot d \equiv 1 \pmod{\phi(n)}$

5. Khóa công khai là (n, e) , khóa bí mật là (n, d) .

Trong thực hành hay chọn $e=65537$

III. Mã hóa công khai

Hệ mật RSA – Mã hóa và giải mã

- Với public key (n, e) và private key (n, d) \rightarrow mã hóa phía người gửi và giải mã phía người nhận.
- Giả sử Bob gửi cho Alice bản rõ M .

Thực hiện mã hóa RSA như sau:

- Chuyển M về số tự nhiên m nằm trong khoảng $(0, n)$ sao cho m, n là hai số nguyên tố cùng nhau

- Mã hóa m thành d như sau:

$$c \equiv m^e \pmod{n}$$

- Sau đó c sẽ được chuyển tới người nhận

Thực hiện giải mã RSA tại người nhận bằng private key (n, d):

Kết quả: $m = c^d \pmod{n}$

Mã hóa RSA

Ví dụ 1:

$$p = 17, q = 11$$

$$\Rightarrow n = pq = 17 * 11 = 187$$

$$\Rightarrow \varphi(n) = 160$$

Chọn $e=7$ vì $\text{UCLN}(7, 160)=1$

Chọn $d=?$ Public key, Private key?

Hệ mật RSA

Ví dụ 1:

Giả sử $m=32$

=> Mã hóa “ m ” bằng RSA

⇒ Bản mật?

$$c = 32 \wedge 5 \% 35 = 2$$

Giải mã c để thu được m ?

$$m = 2 \wedge 29 \% 35 = 32$$

Hệ mật RSA

Ví dụ 2: mã hóa chuỗi nhị phân

Các tham số

Chọn $p=11$ và $q=13$

Khi đó $n=11*13=143$

$$(p-1)(q-1)=120$$

Chọn $e=37$ vì $\gcd(e, 120)=1$

Sử dụng thuật toán gcd để tìm d sao cho
 $e*d-1$ chia hết cho 120 $\rightarrow d=13$

Hệ mật RSA

Ví dụ 2: mã hóa chuỗi nhị phân

Để mã hóa một chuỗi nhị phân gồm các bước:

“Bẻ” thành nhiều đoạn độ dài là u bít sao cho $2^u < 143 \rightarrow u=7$

Mỗi đoạn như vậy sẽ biểu diễn một số nằm trong khoảng 0-127

Tính bản mật Y theo công thức: $Y = X^e \text{ mod } n$

Ví dụ $X=(0000010)=2$, ta có $Y=?$

$Y=106$ hay $Y=(100\ 1010)$ → Bản mật gửi đi là Y

Giải mã? $X=2?$

Hệ mật RSA

Bài tập áp dụng:

Cho bản rõ: $m=65$

$P=41$, $q=43$

Tính n, e, d và bản mật

Thám mã Hệ mật RSA

- ✓ Để giải mã được mã hóa RSA phải tìm được khóa bí mật d. Tức là phần tử nghịch đảo của e modulo $\phi(n)$
- ✓ Để làm được việc này trước hết phải tìm $\phi(n)$
- ✓ Việc tìm giá trị $\phi(n)$ không dễ hơn so với việc phân tích n, vì khi biết $\phi(n)$ và n ta có thể phân tích được $n=p \cdot q$
- ✓ Hệ mã RSA được gọi là an toàn nếu chọn số nguyên tố p,q đủ lớn để việc phân tích thành phần khóa công khai n thành tích 2 thừa số nguyên tố là khó để thực hiện trong thời gian thực

Trao đổi khóa Diffie-Hellman

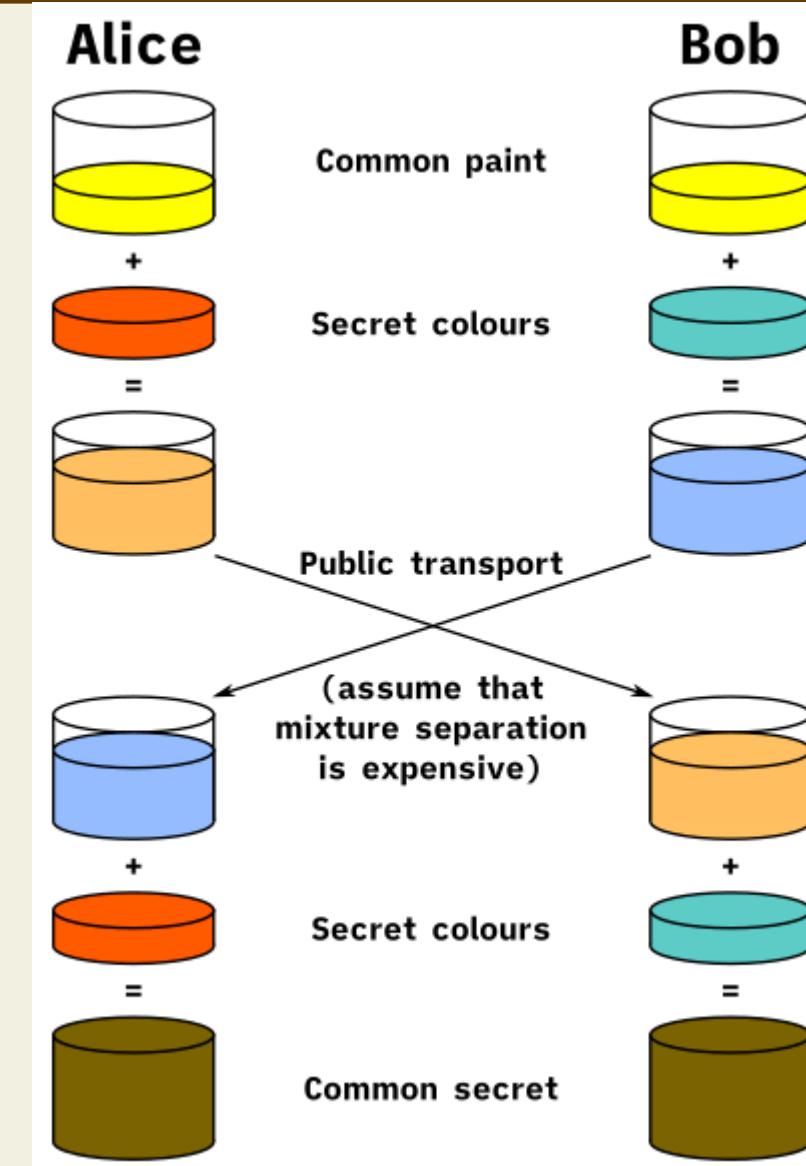
- ✓ Trao đổi khóa Diffie-Hellman là một trong những phát triển quan trọng nhất trong mật mã hóa công khai.
- ✓ Cho phép hai bên trước đây chưa gặp nhau thiết lập một cách an toàn một khóa mà họ có thể sử dụng để bảo mật thông tin liên lạc của họ
- ✓ Trao đổi khóa Diffie-Hellman là thường xuyên được thực hiện trong các giao thức bảo mật như TLS, IPsec, SSH, PGP và nhiều giao thức khác

III. Mã hóa công khai

Trao đổi khóa Diffie-Hellman

Ý tưởng: Alice và Bob trao đổi màu sơn bí mật thông qua hỗn hợp sơn.

- Đầu tiên Alice và Bob trộn màu đã biết chung (màu vàng) với màu bí mật riêng của mỗi người.
- Sau đó, mỗi người chuyển hỗn hợp của mình tới người kia thông qua một kênh vận chuyển công cộng.
- Khi nhận được hỗn hợp của người kia, mỗi người sẽ trộn thêm với màu bí mật của riêng mình và nhận được hỗn hợp cuối cùng.



Quản lý khóa

- Có hai khía cạnh khác biệt đối với việc sử dụng mật mã khóa công khai về vấn đề này:
 - Phân phối khóa công khai
 - Sử dụng hệ thống khóa mã hóa khóa công khai để phân phối khóa bí mật.
- **Phân phối khóa công khai:** một số kỹ thuật được sử dụng để phân phối khóa công khai
 - ✓ Thông báo công khai
 - ✓ Thẩm quyền khóa công khai
 - ✓ Chứng thực khóa công khai
- **Phân phối khóa bí mật sử dụng hệ mật mã khóa công khai:** Mã hóa khóa công khai được dùng để **thiết lập khóa bí mật** cho mỗi phiên trao đổi dữ liệu của **mã hóa đối xứng**. Lúc này khóa bí mật được gọi là khóa phiên (session key), các phiên trao đổi dữ liệu khác nhau sẽ dùng các khóa bí mật khác nhau.

Quản lý khóa

- **Phân phối khóa công khai: Thông báo công khai**

Khi hai người sử dụng muốn truyền dữ liệu với nhau bằng phương pháp mã hóa khóa công khai, trước tiên họ phải trao đổi khóa công khai cho nhau.



Quản lý khóa

- *Phân phối khóa công khai: Thông báo công khai*

Nhược điểm:

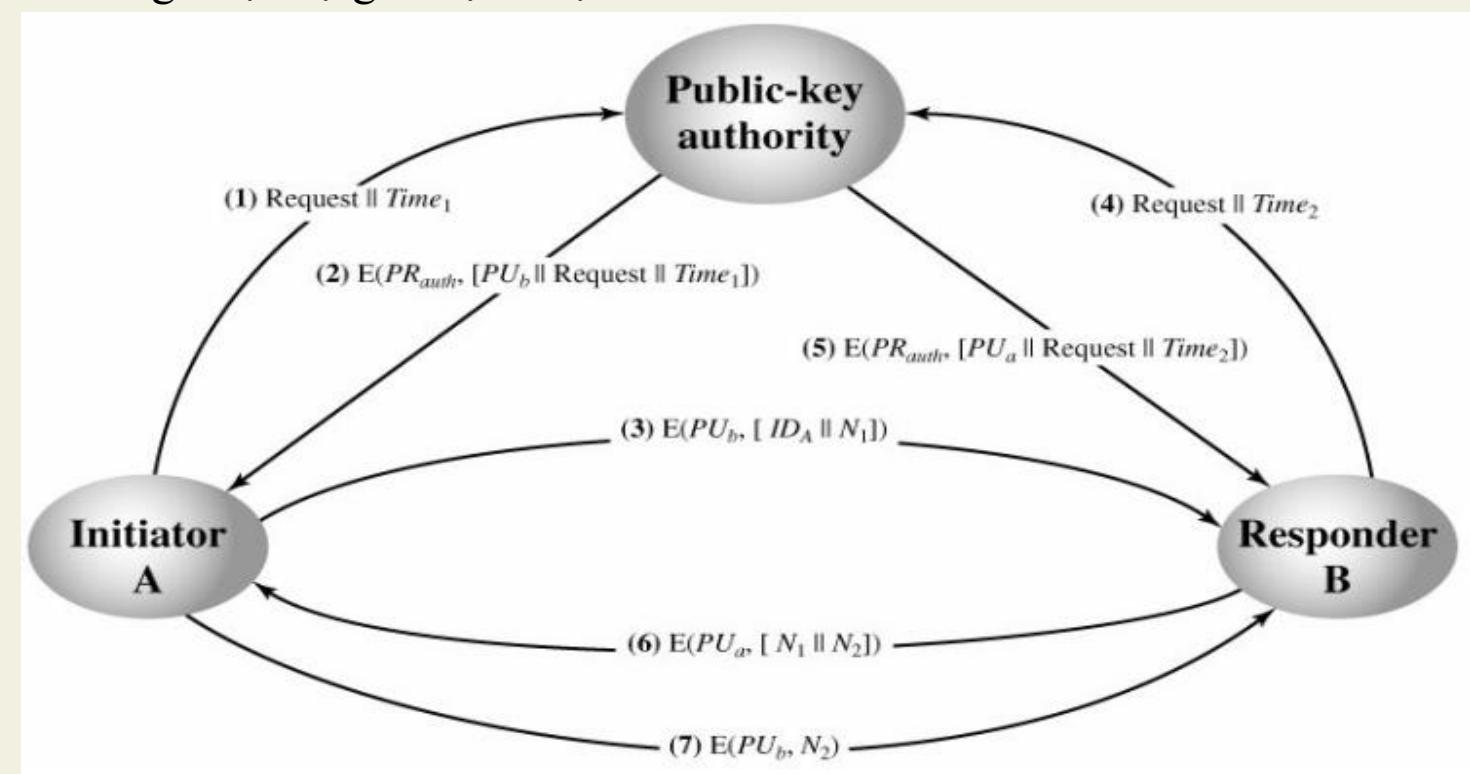
- ✓ Phương pháp trao đổi khóa này rất thuận lợi nhưng có một nhược điểm là bất kỳ ai cũng có thể giả mạo người khác để quảng bá khóa công khai của mình.
- ✓ Tức là, một người dùng bất kỳ có thể giả mạo người dùng A và gửi khóa công khai đến cho các người tham gia khác.
- ✓ Cho tới khi người dùng A phát hiện ra hành vi giả mạo và cảnh báo những người tham gia khác, kẻ giả mạo có thể đọc tất cả các tin nhắn được mã hóa dành cho A và có thể sử dụng các khóa giả mạo để xác thực.

Quản lý khóa

• Phân phối khóa công khai: Thẩm quyền khóa công khai

Phương pháp trao đổi khóa an toàn chống được sự giả mạo được triển khai như hình dưới.

Trung tâm thẩm quyền khóa công khai duy trì một thư mục động chứa khóa công khai của tất cả các người tham gia. Ngoài ra, mỗi người tham gia đều biết khóa công khai của trung tâm và chỉ trung tâm mới biết khóa bí mật (khóa riêng) tương ứng.



Trao đổi khóa công khai thông qua thẩm quyền khóa công khai

Quản lý khóa

• Phân phối khóa công khai: Thẩm quyền khóa công khai

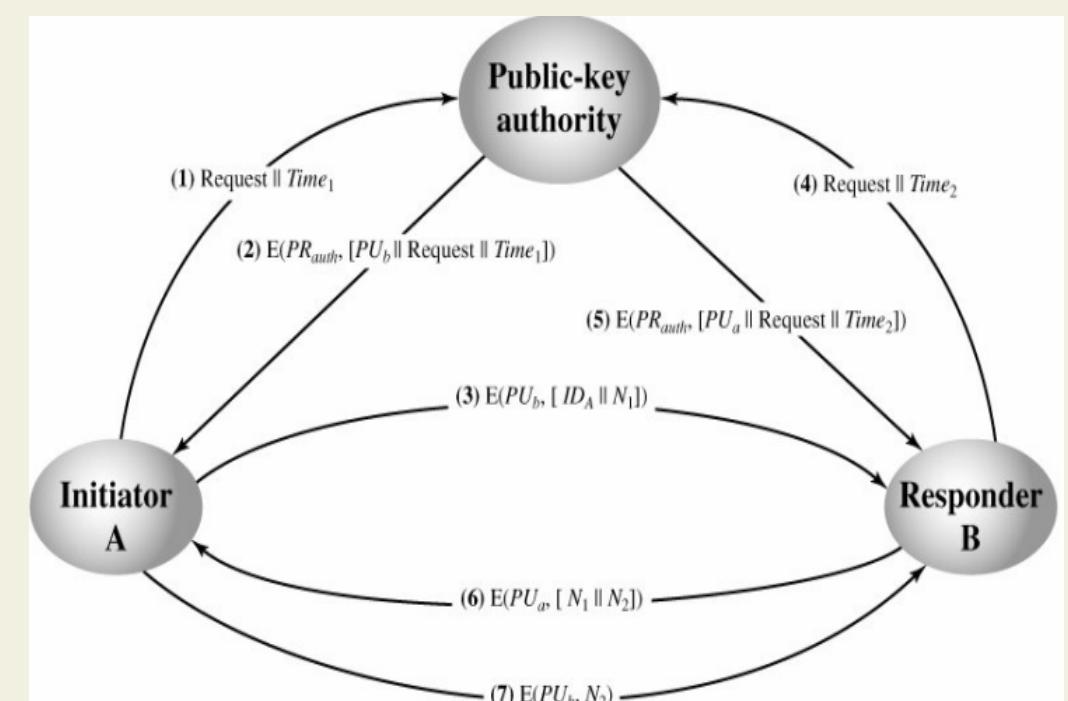
Quá trình trao đổi khóa giữa 2 người A và B thông qua trung tâm được diễn ra các bước như sau (7 bước):

Bước 1: Bên A gửi một thông điệp có gắn thời gian đến trung tâm thẩm quyền để yêu cầu khóa công khai hiện tại của bên B.

Bước 2: Trung tâm thẩm quyền trả lời lại cho A một thông điệp được mã hóa bằng khóa bí mật của mình PR_{auth} . Do đó, bên A có thể giải mã được thông điệp này sử dụng khóa công khai của trung tâm. Nội dung của thông điệp: Khóa công khai của B (PU_b); Yêu cầu Request; Thời gian ban đầu.

Bước 3: A lưu trữ khóa công khai của B và sử dụng nó để mã hóa một thông điệp gửi tới B có chứa số định danh của A (ID_A) và số ngẫu nhiên chỉ sử dụng một lần (N_1) để xác định duy nhất giao dịch này

Bước 4: Bên B nhận khóa công khai của A từ trung tâm có thẩm quyền tương tự như cách mà bên A nhận khóa công khai của B.



Quản lý khóa

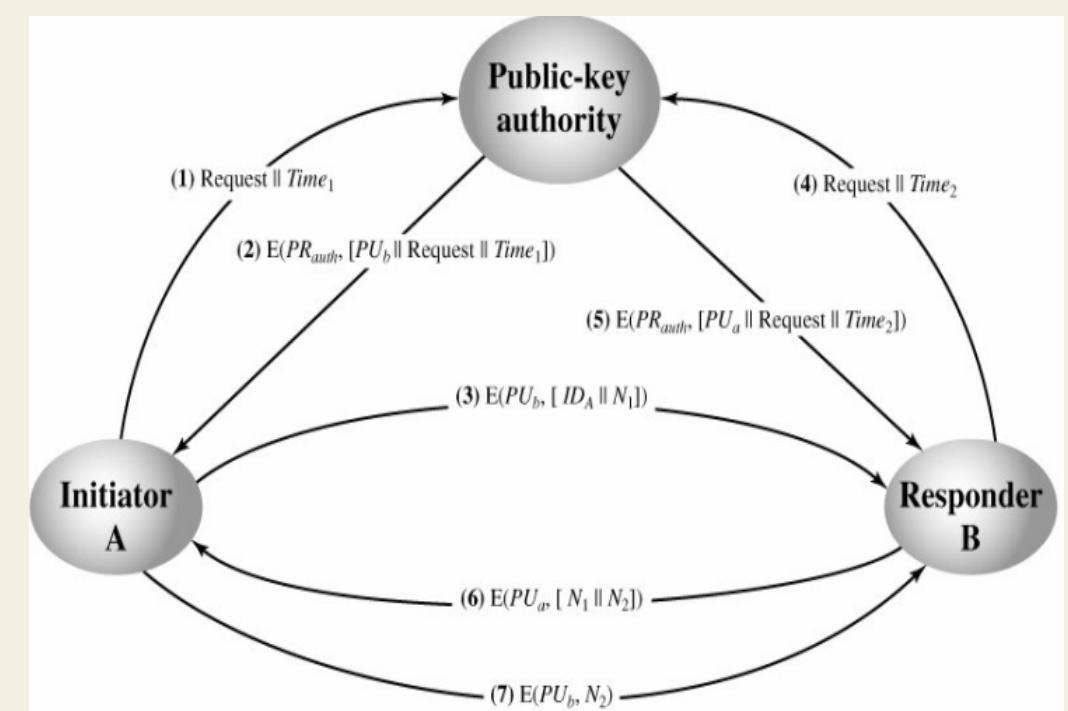
- Phân phối khóa công khai: Thẩm quyền khóa công khai**

Quá trình trao đổi khóa giữa 2 người A và B thông qua trung tâm được diễn ra các bước như sau:

Bước 5: Tại thời điểm này việc phân phối khóa công khai của A và B đã được thực hiện một cách bảo mật, A, B có thể trao đổi thông tin an toàn cho nhau.

Bước 6: Bên B gửi một thông điệp chứa số ngẫu nhiên N_1 nhận được từ A và số ngẫu nhiên N_2 do B tạo đến bên A được mã hóa bằng khóa công khai của A (PU_a).

Bước 7: A trả lại B thông điệp chứa N_2 được mã hóa bằng mã công khai của B (PU_b) để đảm bảo cho B rằng chính là A



Quản lý khóa

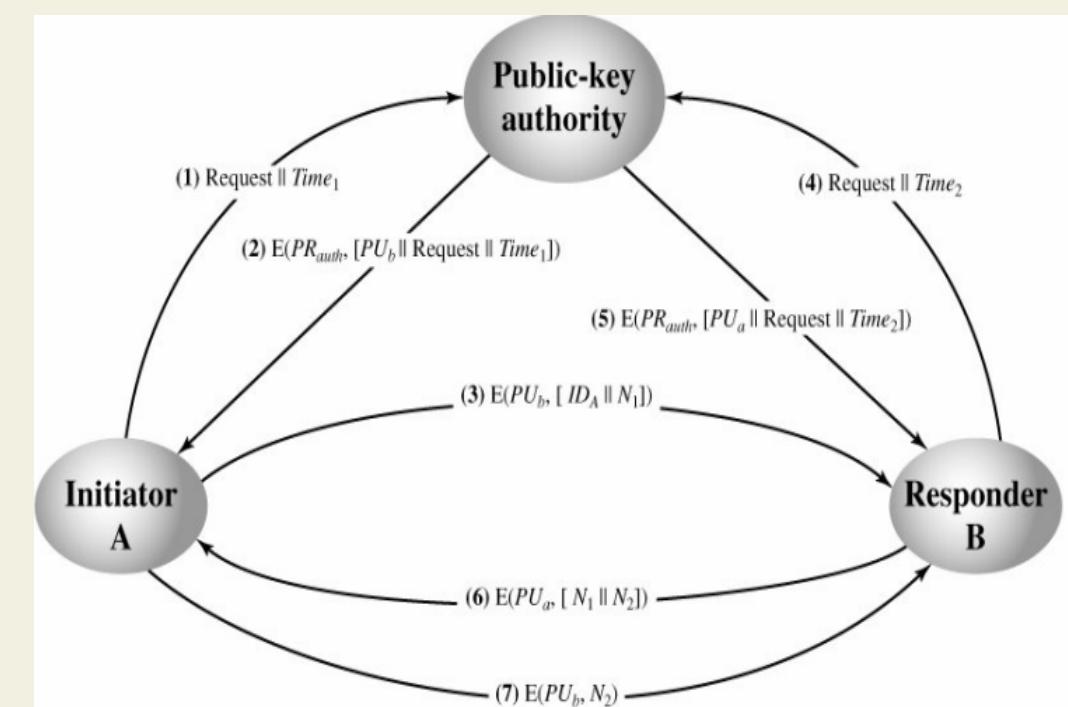
• Phân phối khóa công khai: Chứng thực khóa công khai (public key certificates)

Chứng thực bao gồm khóa công khai ghép với số nhận dạng của chủ sở hữu khóa, toàn bộ thông tin này được ký bởi bên thứ ba đáng tin cậy.

Thông thường, bên thứ ba là cơ quan cấp chứng thực, chẳng hạn như cơ quan chính phủ hoặc tổ chức tài chính, được cộng đồng người dùng tin cậy.

Người dùng có thể gửi khóa công khai của mình cho cơ quan quản lý khóa một cách an toàn và nhận lại chứng thực. Sau đó, người dùng có thể phân phối chứng thực của mình.

Bất kỳ ai cần khóa công khai của người dùng này đều có thể nhận chứng thực và xác minh rằng nó hợp lệ bằng chữ ký đáng tin cậy đính kèm.

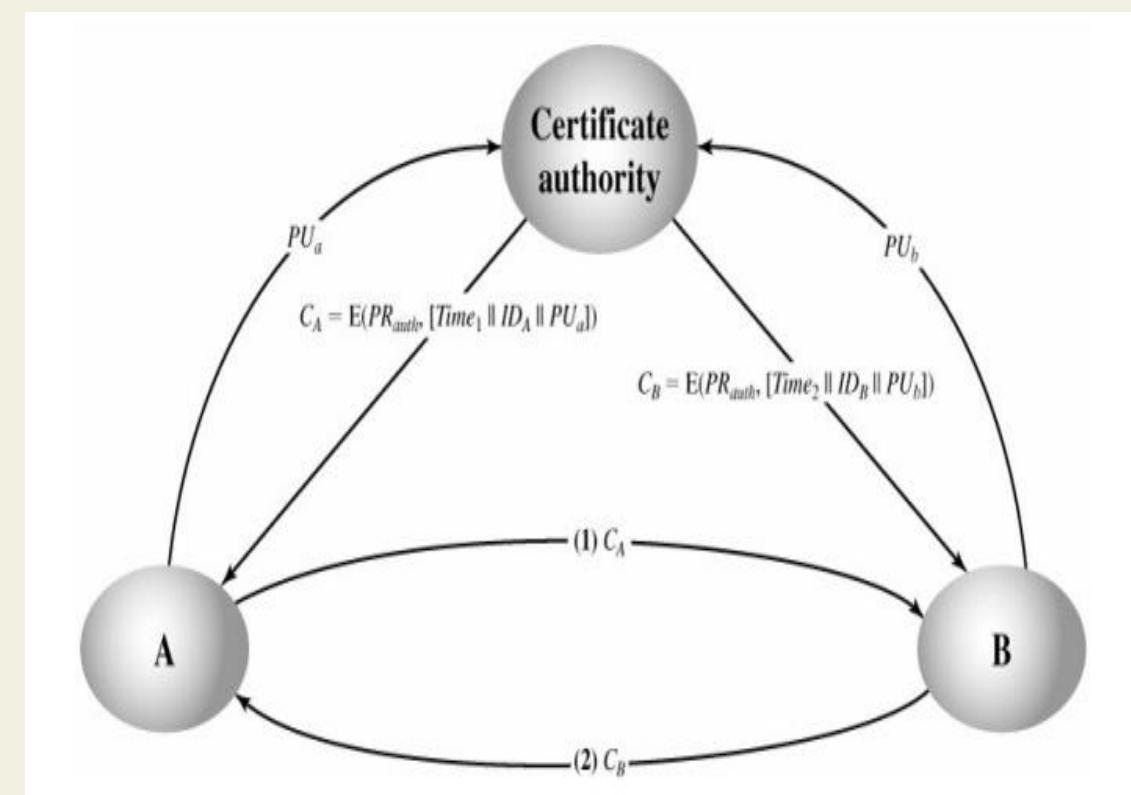


Quản lý khóa

• Phân phối khóa công khai: Chứng thực khóa công khai (public key certificates)

Các bước nhận và phân phối chứng thực được minh họa trên hình bên và các yêu cầu đối với phương pháp trao đổi khóa này như sau:

- **Yêu cầu 1:** Bất kỳ người tham gia nào cũng có khả năng đọc chứng thực để xác định tên và khóa công khai của chủ sở hữu chứng thực.
- **Yêu cầu 2:** Bất kỳ người tham gia nào cũng có thể xác minh rằng chứng thực có nguồn gốc từ cơ quan cấp chứng thực và không phải là giả mạo.
- **Yêu cầu 3:** Chỉ tổ chức phát hành chứng thực mới có thể tạo và cập nhật chứng thực.
- **Yêu cầu 4:** Bất kỳ người tham gia nào cũng có thể xác minh tính hiện thời của chứng thực.



Quản lý khóa

- Phân phối khóa công khai: Chứng thực khóa công khai (public key certificates)**

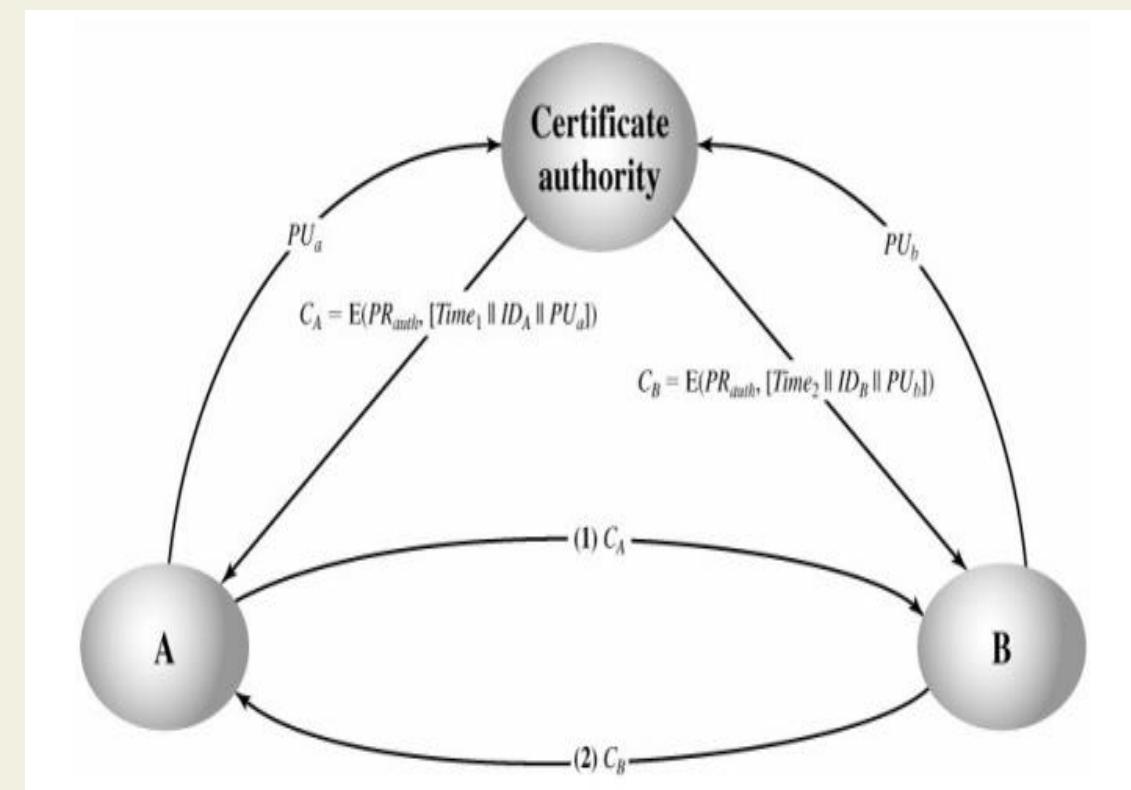
Đối với bên A, tổ chức quản lý chứng thực cung cấp cho chứng thực dưới dạng $C_A = E(PR_{auth}, [T//ID_A//PU_a])$.

Trong đó, PR_{auth} là khóa bí mật của tổ chức cấp chứng thực, T là nhãn thời gian để phản ánh tính hiện thời của chứng thực, ID_A là định danh của A và // là phép ghép.

Sau đó, A có thể chuyển chứng thực này cho bất kỳ người tham gia nào khác, những người này đọc và xác minh chứng thực như sau: $D(PU_{auth}, CA) = D(PU_{auth}, E(PR_{auth}, [T//ID_A//PU_a])) = (T//ID_A//PU_a)$.

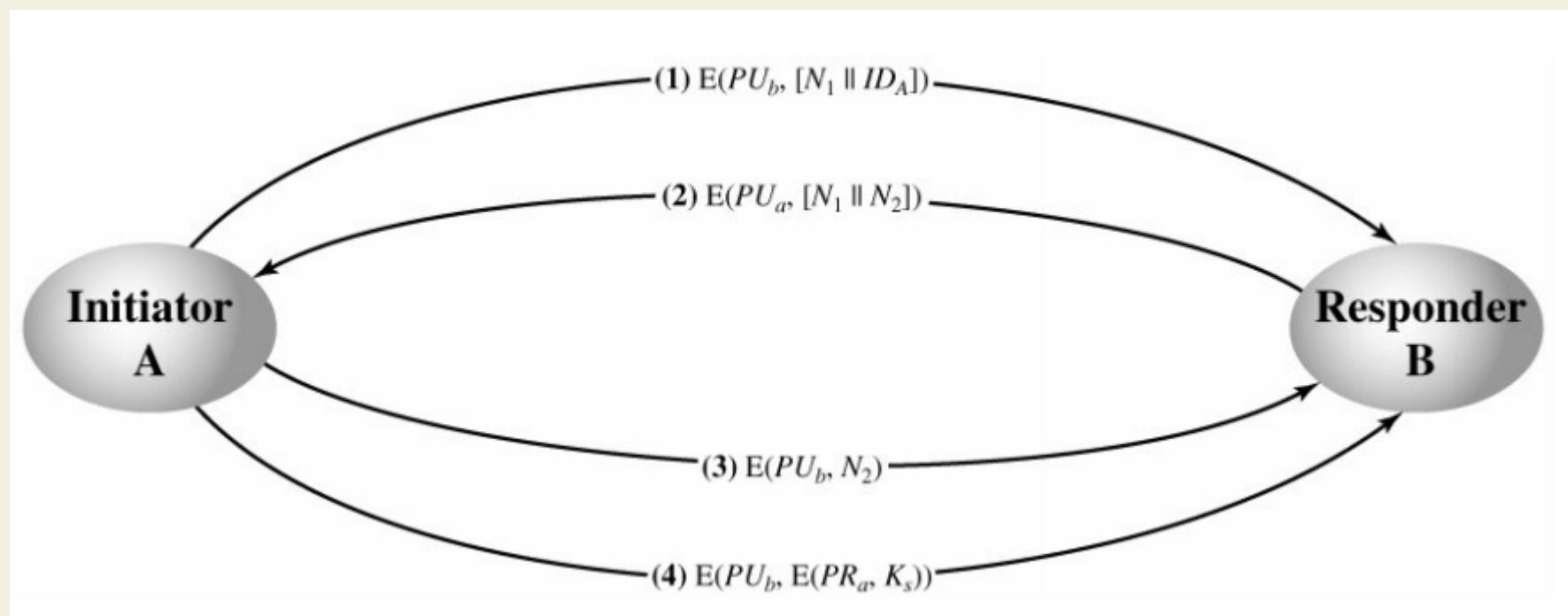
Người nhận sử dụng khóa công khai của tổ chức cấp chứng thực, PU_{auth} để giải mã chứng thực.

Các phần tử IDA và PUA cung cấp cho người nhận tên và khóa công khai của chủ sở hữu chứng chỉ. Nhãn thời gian T xác định tính hiện thời của chứng thực.



Quản lý khóa

- *Phân phối khóa bí mật sử dụng hệ mật mã khóa công khai*
- Mã hóa khóa công khai được dùng để thiết lập khóa bí mật cho mỗi phiên trao đổi dữ liệu. Lúc này khóa bí mật được gọi là khóa phiên (session key), các phiên trao đổi dữ liệu khác nhau sẽ dùng các khóa bí mật khác nhau



Trao đổi khóa bí mật sử dụng hệ mật mã khóa công khai

Quản lý khóa

- Phân phối khóa bí mật sử dụng hệ thống mã hóa công khai**

Quá trình trao đổi khóa bí mật được thực hiện qua các bước sau:

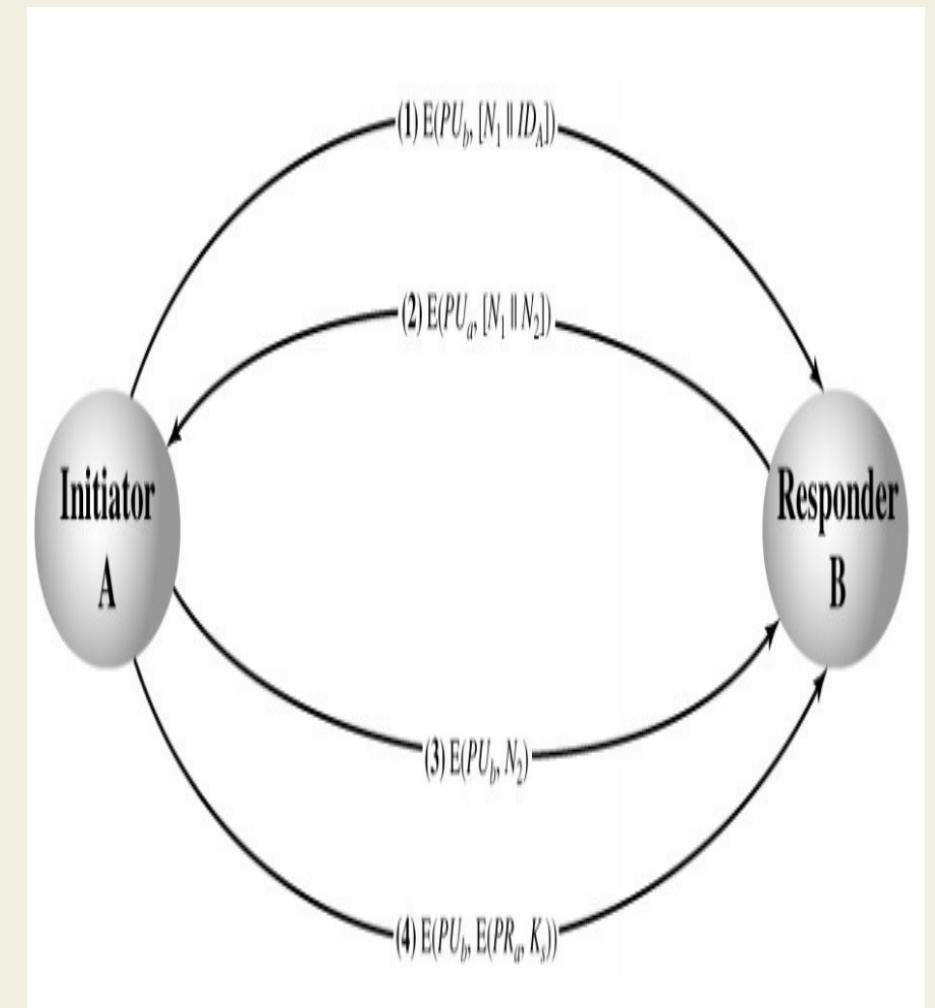
Bước 1: Bên A sử dụng khóa công khai của bên B (PU_b) để mã hóa thông điệp bao gồm một số ngẫu nhiên chỉ sử dụng 1 lần (nonce) N_1 và định danh của A (ID_A).

Bước 2: Bên B gửi một thông điệp đến bên A bao gồm số ngẫu nhiên sử dụng 1 lần của A (N_1), cùng một số ngẫu nhiên mới được tạo bởi B (N_2) được mã hóa bằng khóa công khai của A (PU_a). Bởi vì chỉ có B mới có thể giải mã được thông điệp (1) do A gửi, sự hiện diện của N_1 trong thông điệp (2) đảm bảo cho A rằng chính là B.

Bước 3: Bên A trả về cho bên B thông điệp chứa N_2 được mã hóa bằng mã công khai của B (PU_b) để đảm bảo cho B rằng thông điệp này do A gửi.

Bước 4: Bên A lựa chọn khóa bí mật K_s và gửi thông điệp được mã hóa $M = E(PU_b, E(PR_a, K_s))$ cho B. Mã hóa thông điệp bằng mã công khai của B để đảm bảo rằng chỉ B mới có thể đọc được, mã hóa bằng khóa riêng của A (PR_a) để đảm bảo rằng chỉ có A mới có thể gửi thông điệp này.

Bước 5: B giải mã để khôi phục lại khóa bí mật K_s



Quản lý khóa

- **Trao đổi khóa Diffie Hellman**

Mục đích của thuật toán là để hai người dùng có thể trao đổi khóa một cách an toàn và khóa này được sử dụng để mã hóa cho các thông điệp trao đổi sau đó. Thuật toán được thực hiện như sau:

- Đầu tiên 2 bên sử dụng công khai số nguyên tố q và a là primary root của q . Tiếp theo, bên A chọn một số nguyên ngẫu nhiên $X_A < q$ và tính $Y_A = a^{X_A} \text{ mode } q$.
- Tương tự, bên B chọn một số ngẫu nhiên $X_B < q$ và tính $Y_B = a^{X_B} \text{ mode } q$.
- Cả 2 bên giữ X bí mật và gửi Y công khai cho nhau.
- Cuối cùng, bên A tính được khóa $K_A = (Y_B)^{X_A} \text{ mode } q$ và B tính được $'K_B = (Y_A)^{X_B} \text{ mode } q$. Hai giá trị K_A và K_B tính được là trùng nhau

$$K_A = (Y_B)^{X_A} \text{ mod } q = (\alpha^{X_B} \text{ mod } q)^{X_A} \text{ mod } q = (\alpha^{X_B})^{X_A} \text{ mod } q = \alpha^{X_A \cdot X_B} \text{ mod } q$$

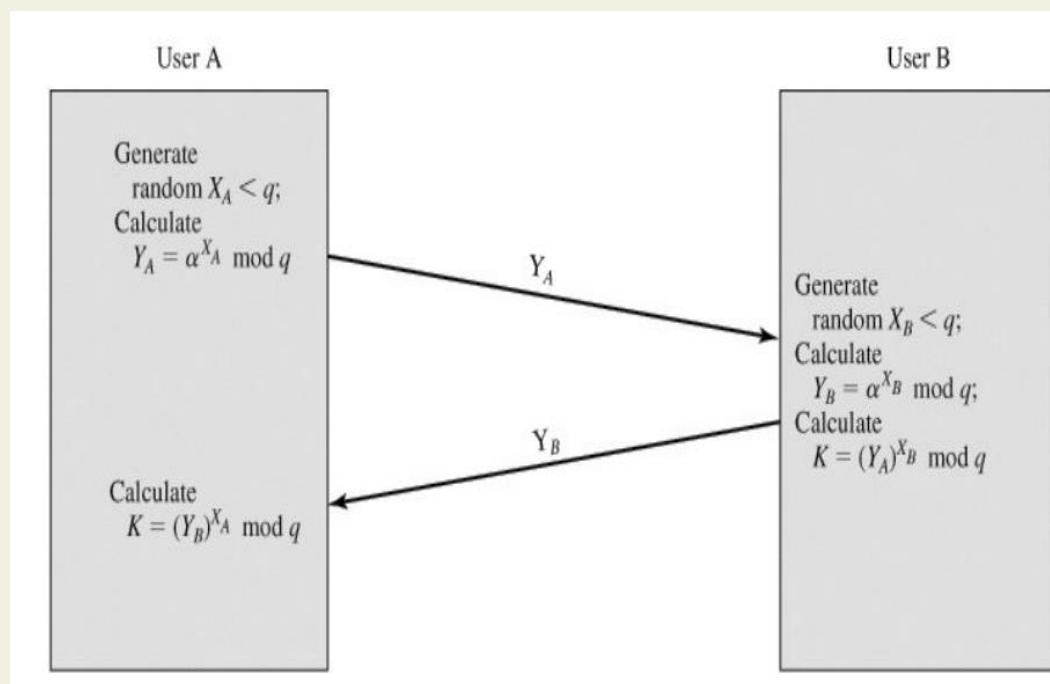
$$K_B = (Y_A)^{X_B} \text{ mod } q = (\alpha^{X_A} \text{ mod } q)^{X_B} \text{ mod } q = (\alpha^{X_A})^{X_B} \text{ mod } q = \alpha^{X_A \cdot X_B} \text{ mod } q$$

Khóa K này có thể sử dụng làm khóa bị mất cho thuật toán mã hóa đối xứng

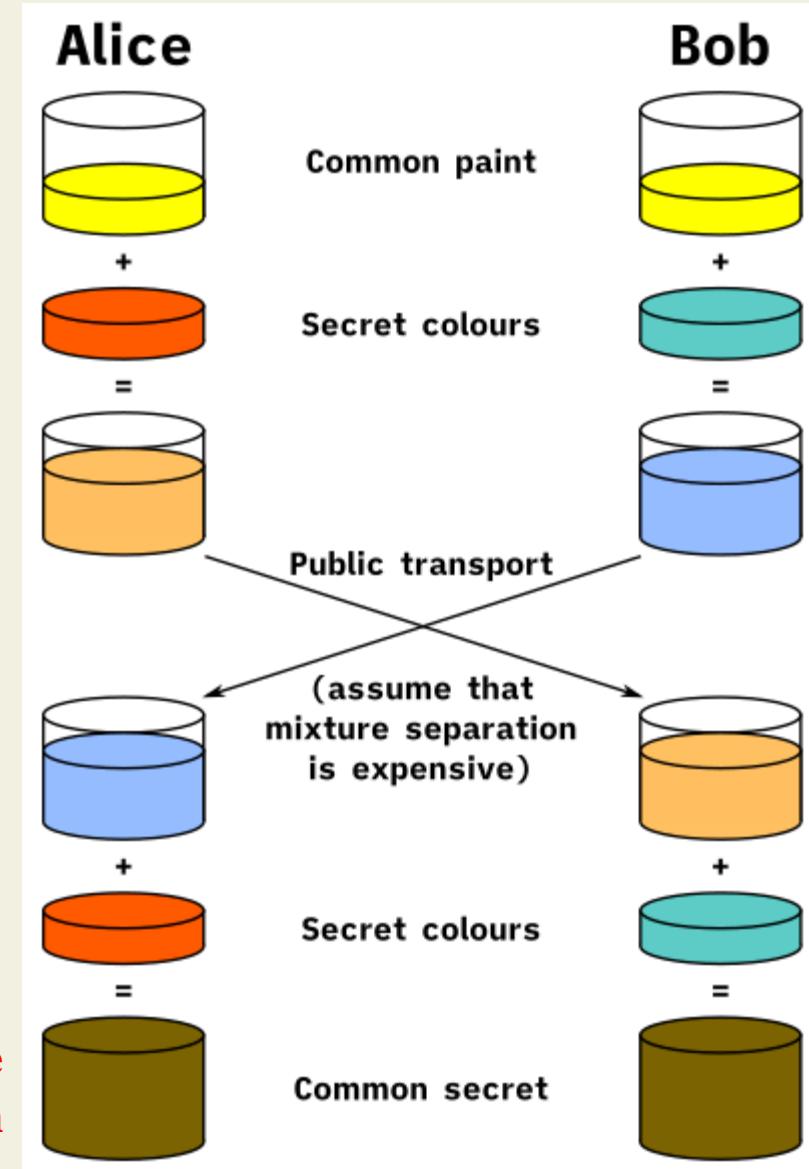
Quản lý khóa

• Trao đổi khóa Diffie Hellman

Minh họa



Tuy nhiên, phương pháp trao đổi khóa theo thuật toán Diffie Hellman không chống được hình thức tấn công kẻ ở giữa (man in the middle attack)



III. Mã hóa công khai

Một câu hỏi khá thú vị là có thể đảo vai trò của public key và private key hay không?

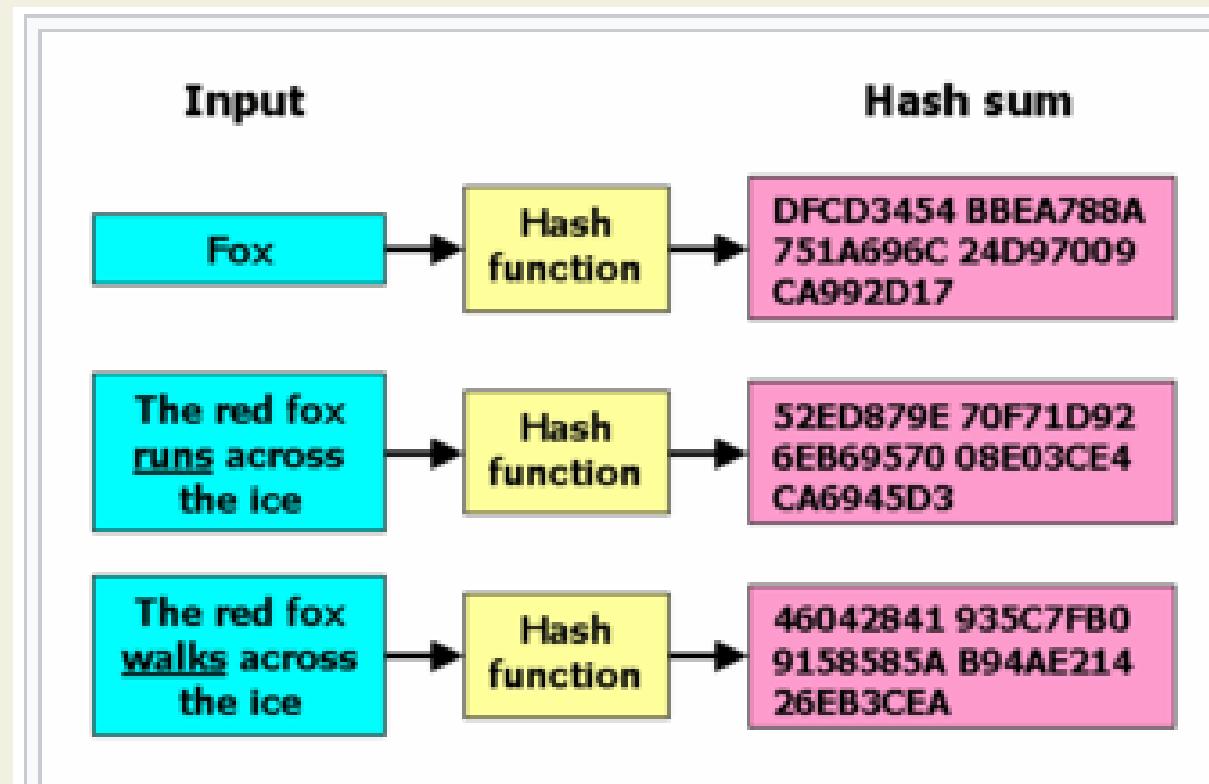
Chữ ký số - Digital signature

Cryptographic Hash – Hàm băm mật mã

- *Cryptographic hash function*) là một hàm băm với một số tính chất bảo mật nhất định để phù hợp việc sử dụng trong nhiều ứng dụng bảo mật thông tin đa dạng, chẳng hạn như chứng thực (authentication) và kiểm tra tính nguyên vẹn của thông điệp (*message integrity*)
- Một hàm băm nhận đầu vào là một xâu ký tự dài (hay *bản tin*) có độ dài tùy ý và tạo ra kết quả là một xâu ký tự có độ dài cố định
- Một số hàm băm thông dụng: **MD5, SHA-1**

Cryptographic Hash – Hàm băm mật mã

- Ví dụ:



Chữ ký số sử dụng RSA

- Việc ký tên và xác thực chữ ký số sử dụng hệ mã hóa RSA tương tự như quá trình mã hóa mà giải mã ở trên
- Tuy nhiên vai trò của public key và private thì có thay đổi
- Để tạo chữ ký, người gửi sẽ dùng private key và người nhận sẽ dùng public key để xác thực chữ ký đó.
- Tuy nhiên, vì bản tin rất dài nên việc mã hóa toàn bộ bản tin sẽ rất mất thời gian
- Chữ ký số thường sử dụng phương pháp mã hóa giá trị **hash** của bản tin.

Chữ ký số sử dụng RSA

- Các hàm hash là hàm 1 chiều, vì vậy dù có được hash cũng không thể biết được bản tin gốc
- Độ dài hash là cố định và thường rất nhỏ, vì vậy chữ số sẽ không chiếm quá nhiều dung lượng
- Giá trị hash còn có thể dùng để kiểm tra lại bản tin nhận được có nguyên vẹn hay không?
- Chữ ký số đem lại nhiều giá trị hơn chữ ký tay rất nhiều
- Việc xử lý chữ ký số phức tạp hơn hẳn chữ ký tay truyền thống.

Chữ ký số sử dụng RSA

Xác định nguồn gốc

- Hệ mã hóa bắt đối xứng cho phép tạo chữ ký với private key mà chỉ người sở hữu chữ ký mới biết.
- Khi nhận gói tin:
 - Người nhận xác thực chữ ký bằng cách dùng public key giải mã,
 - Sau đó tính giá trị hash của bản tin gốc và so sánh với hash trong gói tin nhận được,
 - Hai chuỗi này phải trùng khớp với nhau

Chữ ký số sử dụng RSA

Dữ liệu được giữ một cách toàn vẹn

- Tin nhắn gửi từ chủ private key rất khó có thể bị giả mạo
- Không thể thay đổi tin nhắn được vì không có private key để sửa đổi chữ ký số cho phù hợp.

Chữ ký số không thể phủ nhận

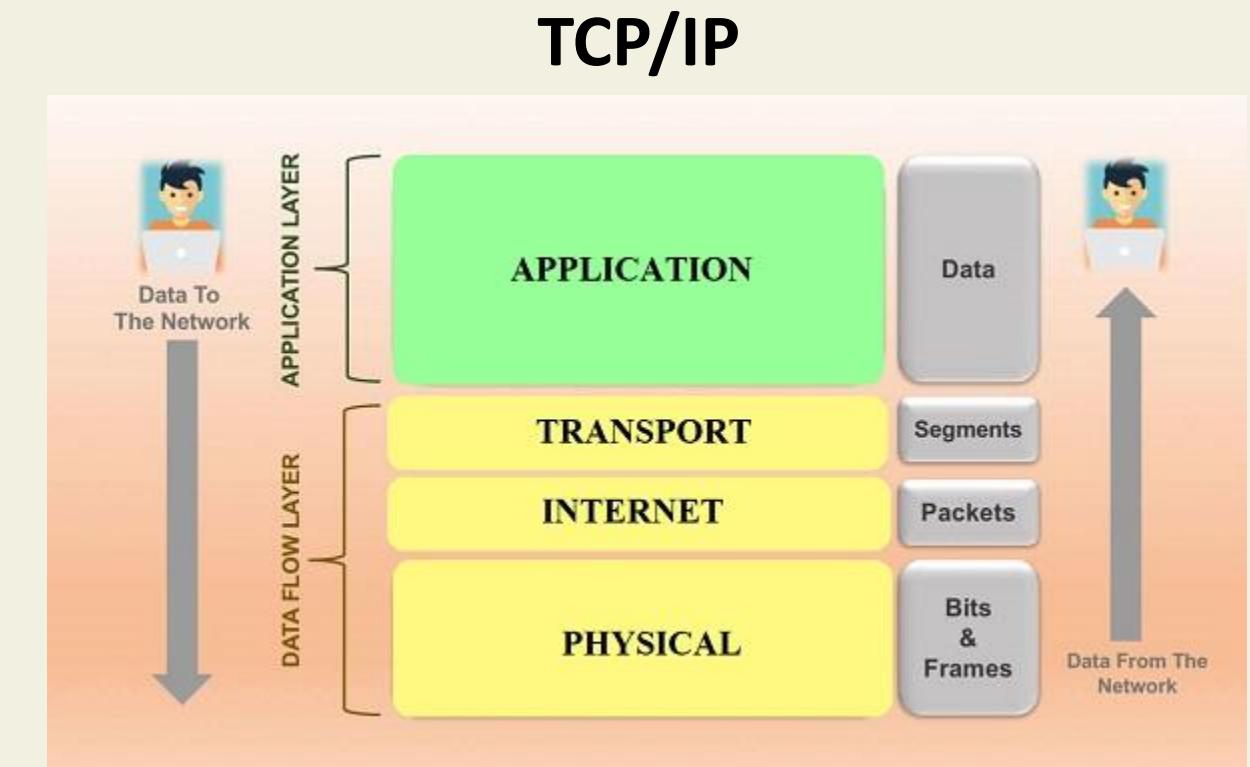
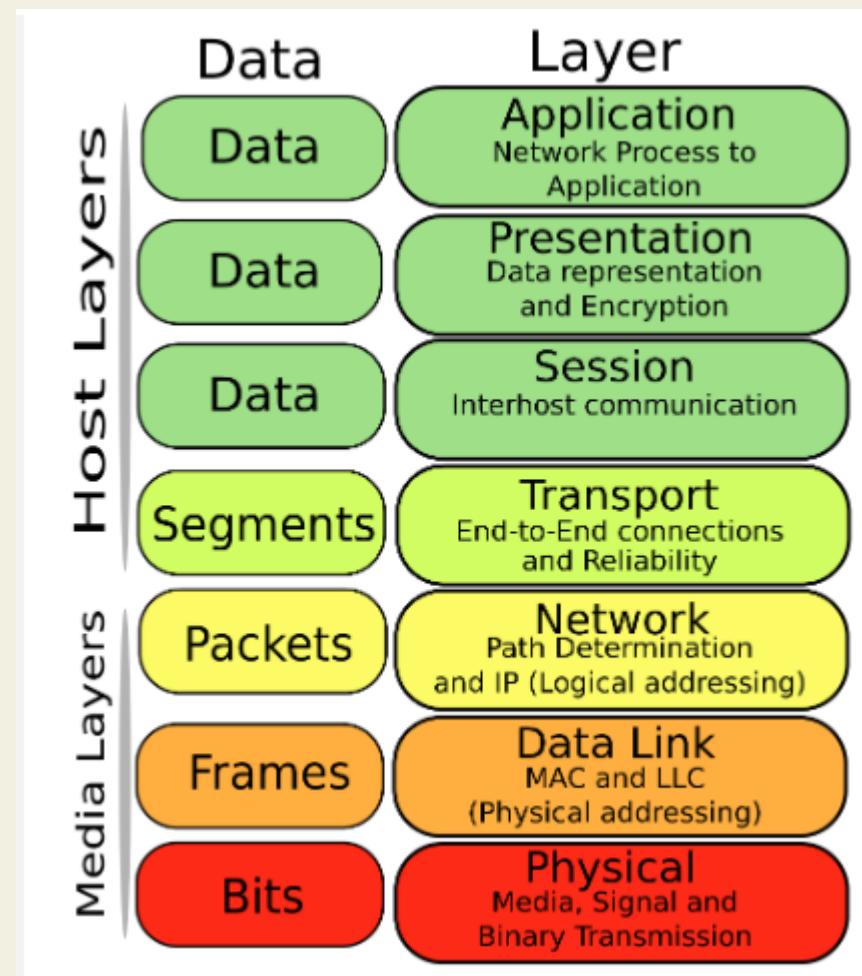
- Trong giao dịch, một gói tin kèm chữ ký số rất dễ dàng tìm ra được nguồn gốc của chữ ký đó.
- Bởi vì private key là bí mật và chỉ người chủ của nó mới có thể biết, họ không thể chối cãi rằng chữ ký này không phải do họ phát hành

Câu hỏi ôn tập

1. Nêu các đặc điểm của DES, và so sánh với 3-DES, AES?
2. So sánh ưu nhược điểm của mã hóa bí mật và mã hóa công khai?
3. Ứng dụng của AES và RSA?
4. Hàm hash một chiều là gì? Ứng dụng của hash-function?
5. Thuật toán trao đổi khóa Diffie-Hellman không an toàn trước các cuộc tấn công Man-in-the-Middle như thế nào?

An ninh tầng giao vận (Transport –Level security)

An ninh tầng giao vận (Transport –Level security)



Giới thiệu về SSL

- SSL (Secure Socket Layer) là dịch vụ an toàn tầng vận chuyển (transport layer) được phát triển bởi Netscape
- SSL cung cấp khả năng mã hóa để bảo mật các kết nối giữa máy khách và máy chủ
- SSL có thể sử dụng để hỗ trợ các giao dịch an toàn cho rất nhiều ứng dụng khác nhau trên Internet.

Nhiệm vụ:

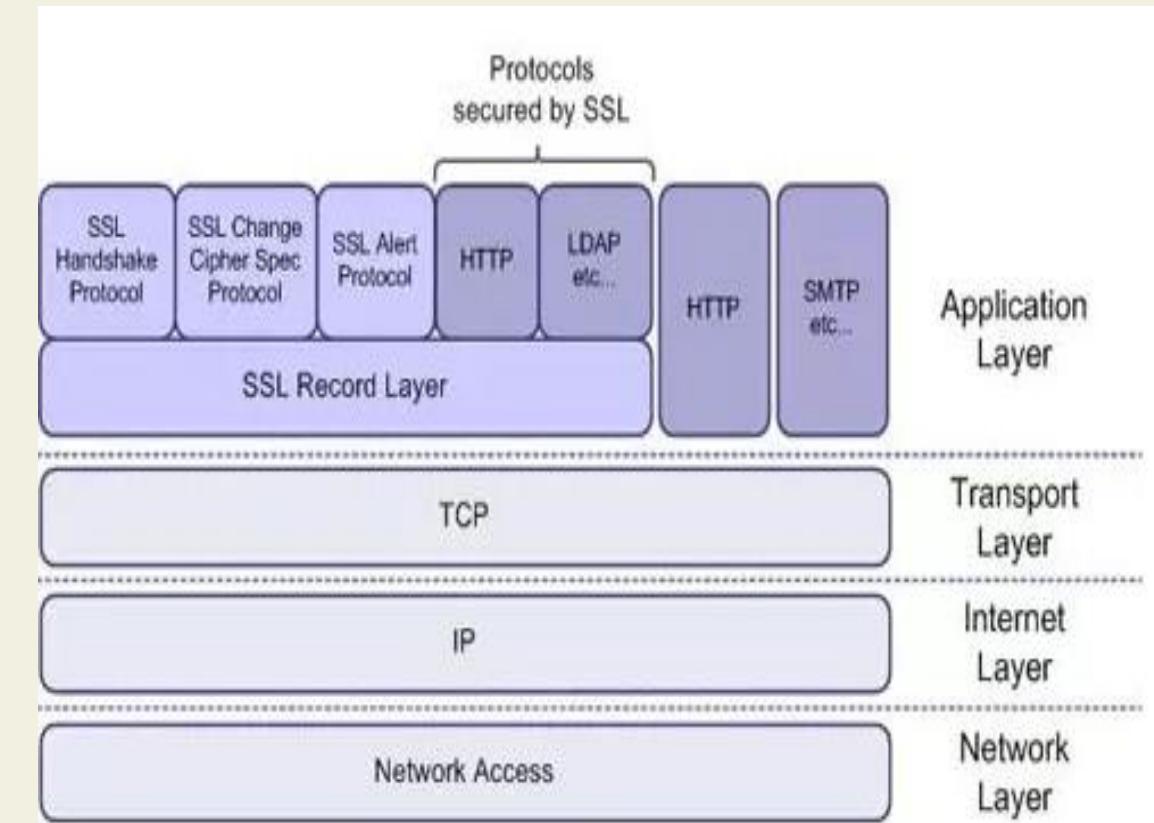
Xác thực máy chủ: cho phép người sử dụng xác thực được máy chủ muốn kết nối. Lúc này, phía browser sử dụng các kỹ thuật mã hoá công khai để chắc chắn rằng chứng chỉ và khoá công khai của máy chủ là có giá trị và được cấp phát bởi một CA trong danh sách các CA đáng tin cậy của máy trạm

Xác thực máy trạm: cho phép phía máy chủ xác thực được người sử dụng muốn kết nối. Phía máy chủ cũng sử dụng các kỹ thuật mã hoá công khai để kiểm tra xem chứng chỉ và khoá công khai của máy chủ có giá trị hay không và được cấp phát bởi một CA trong danh sách các CA đáng tin cậy không.

Mã hoá kết nối: tất cả các thông tin trao đổi giữa máy trạm và máy chủ được mã hoá trên đường truyền nhằm nâng cao khả năng bảo mật.

• Cấu trúc của giao thức SSL:

- ✓ Các bên giao tiếp (nghĩa là client và server) có thể xác thực nhau bằng cách sử dụng mật mã khóa chung
- ✓ Sự bí mật của lưu lượng dữ liệu được bảo vệ vì nối kết được mã hóa trong suốt sau khi một sự thiết lập quan hệ ban đầu và sự thương lượng khóa session đã xảy ra.
- ✓ Tính xác thực và tính toàn vẹn của lưu lượng dữ liệu cũng được bảo vệ vì các thông báo được xác thực và được kiểm tra tính toàn vẹn một cách trong suốt bằng cách sử dụng MAC.



Giới thiệu về SSL

- Hoạt động của SSL dựa trên hai nhóm con giao thức là giao thức “bắt tay” và giao thức “bản ghi”. Các bước thực hiện trong quá trình bắt tay như sau:

1. **Máy trạm sẽ gửi cho máy chủ số phiên bản SSL** đang dùng, các tham số của thuật toán mã hoá, dữ liệu được tạo ra ngẫu nhiên (chữ ký số) và một số thông tin khác mà máy chủ cần để thiết lập kết nối với máy trạm.
2. **Máy chủ gửi cho máy trạm số phiên bản SSL** đang dùng, các tham số của thuật toán mã hoá, dữ liệu được tạo ra ngẫu nhiên và một số thông tin khác mà máy trạm cần để thiết lập kết nối với máy chủ
3. **Máy trạm sử dụng một số thông tin mà máy chủ gửi đến để xác thực máy chủ**
4. **SD tất cả các thông tin được tạo ra trong giai đoạn bắt tay ở trên, máy trạm (cùng với sự cộng tác của máy chủ và phụ thuộc vào thuật toán được sử dụng)** sẽ tạo ra premaster secret cho phiên làm việc, mã hoá bằng khoá công khai mà máy chủ gửi đến trong chứng chỉ ở bước 2, và gửi đến máy chủ.
5. **Nếu máy chủ có yêu cầu xác thực máy trạm**, thì phía máy trạm sẽ đánh dấu vào phần thông tin riêng chỉ liên quan đến quá trình “bắt tay” này mà hai bên đều biết.
6. **Máy chủ sẽ xác thực máy trạm.** Trường hợp máy trạm không được xác thực, phiên làm việc sẽ bị ngắt. Còn nếu máy trạm được xác thực thành công, máy chủ sẽ sử dụng khoá bí mật để giải mã premaster secret, sau đó thực hiện một số bước để tạo ra master secret

Giới thiệu về SSL

7. Máy trạm và máy chủ sẽ sử dụng master secret để tạo ra các khóa phiên, đó chính là các khoá đối xứng được sử dụng để mã hoá và giải mã các thông tin trong phiên làm việc và kiểm tra tính toàn vẹn dữ liệu

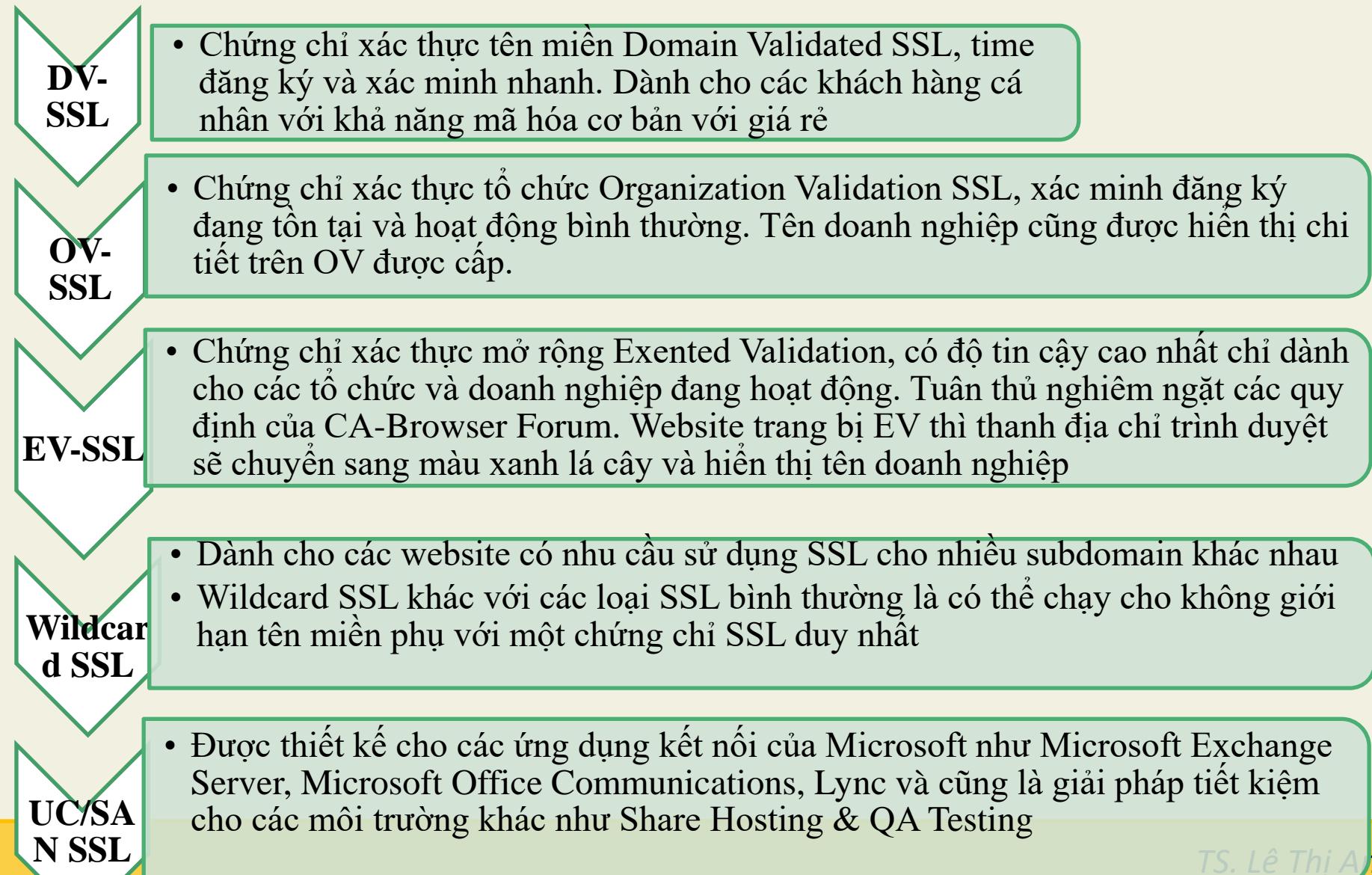
8. Máy trạm sẽ gửi thông báo đến máy chủ thông báo rằng các thông điệp tiếp theo sẽ được mã hoá bằng khoá phiên. Sau đó nó gửi một lời nhắn đã được mã hoá để thông báo rằng phía máy trạm đã kết thúc giai đoạn “bắt tay”

9. Máy chủ gửi lại thông báo đến máy trạm thông báo rằng các thông điệp tiếp theo sẽ được mã hoá bằng khoá phiên. Sau đó nó gửi một lời nhắn đã được mã hoá để thông báo rằng máy chủ đã kết thúc giai đoạn “bắt tay”.

10. Lúc này giai đoạn “bắt tay” đã hoàn thành, và phiên làm việc SSL bắt đầu. Cả hai phía máy trạm và máy chủ sẽ sử dụng các khoá phiên để mã hoá và giải mã thông tin trao đổi giữa hai bên, kiểm tra tính toàn vẹn dữ liệu

Phân loại chứng chỉ SSL

- Các loại chứng chỉ SSL được sử dụng ở Việt Nam:



Lợi ích về An toàn bảo mật khi sử dụng chứng chỉ SSL

Chứng chỉ bảo mật SSL đã đem lại rất nhiều lợi ích về bảo mật cho website và trình duyệt web của người dùng

- ✓ Xác thực website, giao dịch.
- ✓ Nâng cao hình ảnh, thương hiệu và uy tín doanh nghiệp
- ✓ Bảo mật các giao dịch giữa khách hàng và doanh nghiệp, các dịch vụ truy nhập hệ thống
- ✓ Bảo mật webmail và các ứng dụng như Outlook Web Access, Exchange và Office Communication Server
- ✓ Bảo mật các ứng dụng ảo hóa như Citrix Delivery Platform hoặc các ứng dụng điện toán đám mây
- ✓ Bảo mật dịch vụ FTP
- ✓ Bảo mật truy cập control panel
- ✓ Bảo mật các dịch vụ truyền dữ liệu trong mạng nội bộ, file sharing, extranet
- ✓ Bảo mật VPN Access Servers, Citrix Access Gateway

- **Giao thức TLS:** là sự kế thừa và thay thế SSL

- TLS protocol là một giao thức quan trọng để bảo mật các kết nối mạng trực tuyến.
- Các kết nối này được bảo mật bằng cách sử dụng mật mã đối xứng để mã hóa dữ liệu truyền đi
- Các keys được tạo ra duy nhất cho mỗi kết nối và dựa trên một chia sẻ bí mật ở đầu phiên kết nối gọi là TLS handshake
- TLS protocol được sử dụng rộng rãi trên Internet để bảo vệ các giao tiếp dữ liệu giữa client and server, bao gồm cả trang web, email và các dịch vụ mạng khác.
- TLS là sự kế thừa cho SSL (Secure Sockets Layer)
- Có thể nói rằng giao thức TLS v1.0 được phát triển dựa trên giao thức SSL v3.0 nhưng giữa chúng có những điểm khác biệt

- **Chức năng của giao thức của TLS:**
- Chức năng chính của giao thức TLS là cung cấp sự riêng tư bảo đảm sự nguyên vẹn cho dữ liệu giữa hai ứng dụng trong môi trường mạng.
- Vì TLS là giao thức được phát triển từ giao thức SSL nên giao thức TLS cũng theo mô hình client-server.
- Trong mô hình TCP/IP thì giao thức TLS gồm có hai lớp: Lớp Record Layer và lớp Handshake Layer.
- Record layer là lớp thấp nhất gồm TLS record protocol (trên tầng giao vận như giao thức điều khiển truyền tải TCP, giao thức truyền vận không tin cậy UDP).

- **Chức năng của giao thức của TLS:**
- Tính năng kết nối riêng tư: ứng dụng mã hoá đối xứng được sử dụng để mã hoá dữ liệu (mã hoá AES...).
- Các khoá để mã hoá đối xứng được sinh ra trong mỗi lần thực hiện kết nối, được thỏa thuận bí mật của giao thức khác (ví dụ TLS).
- Nhờ vậy mà giao thức TLS có thể được sử dụng mà không cần mã hoá.
- Tính năng kết nối đáng tin cậy: Một thông điệp vận chuyển thông báo sẽ bao gồm kiểm tra tính toàn vẹn (sử dụng hàm Băm ví dụ SHA-1).
- Không chỉ có vậy, giao thức TLS còn có thể sử dụng để đóng gói, mã hoá dữ liệu, phân mảnh, hỗ trợ các máy chủ nhận ra nhau để từ đó tiến hành thỏa thuận mã hóa.

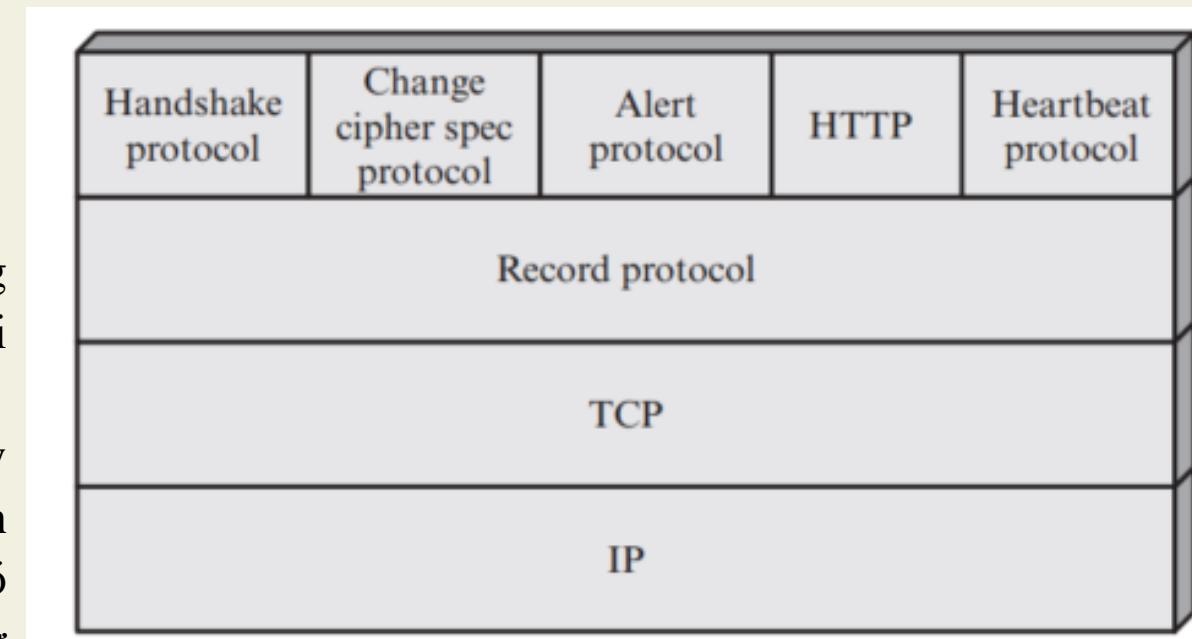
- **Cấu trúc TLS:**

TLS được thiết kế để sử dụng TCP nhằm cung cấp dịch vụ bảo mật đầu cuối đáng tin cậy

Hai khái niệm TLS quan trọng là phiên TLS (session) và kết nối TLS (connection)

- Kết nối: Đối với TLS, các kết nối là mối quan hệ ngang hàng. Các kết nối là tạm thời. Mỗi kết nối được liên kết với một phiên.
- Phiên: Phiên TLS là sự kết hợp giữa máy khách và máy chủ. Các phiên được tạo bởi Giao thức bắt tay. Các phiên xác định một tập hợp các tham số bảo mật bằng mật mã, có thể được chia sẻ giữa nhiều kết nối. Các phiên được sử dụng để tránh thương lượng tốn kém các tham số bảo mật mới cho mỗi kết nối.

Về cơ bản, kiến trúc của TLS cũng tương tự như SSL. Tuy nhiên, có bổ sung thêm Heartbeat Protocol

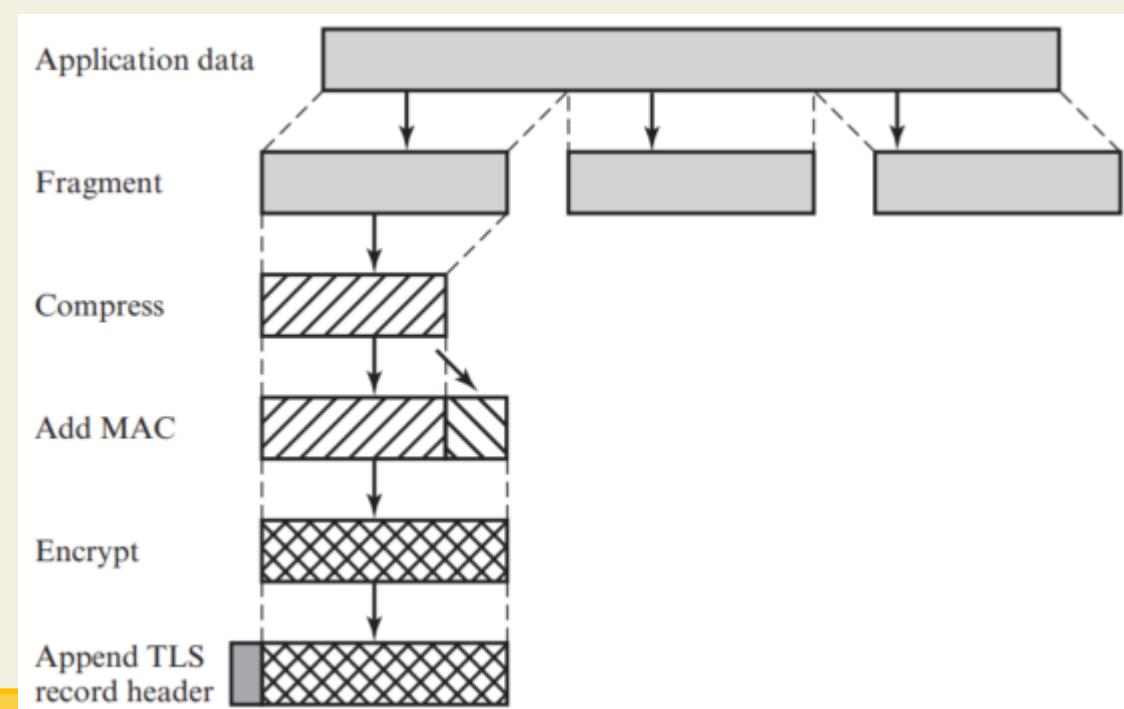


- **Cấu trúc TLS:**

Giao thức TLS Record: cung cấp hai dịch vụ cho các kết nối TLS

Tính bí mật: Giao thức bắt tay xác định một khóa bí mật dùng chung được sử dụng để mã hóa thông thường các tải trọng TLS

Tính toàn vẹn của thông báo: Giao thức bắt tay cũng xác định khóa bí mật dùng chung được sử dụng để tạo mã xác thực tin nhắn (MAC).



- **Cấu trúc TLS:**

Alert Record: cung cấp hai dịch vụ cho các kết nối TLS

- ✓ Giao thức cảnh báo được sử dụng để truyền các cảnh báo liên quan đến TLS đến thực thể ngang hàng
- ✓ Các thông báo cảnh báo được nén và mã hóa, như được chỉ định bởi trạng thái hiện tại
- ✓ Mỗi thông báo trong giao thức này bao gồm hai byte (Hình dưới). Byte đầu tiên nhận giá trị cảnh báo (1) hoặc nghiêm trọng (2) để truyền tải mức độ nghiêm trọng của thông báo.
- ✓ Nếu mức độ nghiêm trọng, TLS sẽ ngay lập tức chấm dứt kết nối
- ✓ Các kết nối khác trong cùng một phiên có thể tiếp tục, nhưng không có kết nối mới nào trong phiên này có thể được thiết lập.

- **Cấu trúc TLS:**

Alert Record:

Byte thứ hai chứa mã cho biết cảnh báo cụ thể.

- unexpected_message: Đã nhận được một tin nhắn không phù hợp.
- bad_record_mac: Đã nhận được MAC không chính xác.
- ecompression_failure: Chức năng giải nén nhận đầu vào không đúng (ví dụ: không thể giải nén hoặc giải nén lớn hơn mức tối đa cho phép chiều dài).
- handshake_failure: Người gửi không thể thương lượng một bộ tham số bảo mật có thể chấp nhận được với các tùy chọn có sẵn.
- invalid_parameter: Một trường trong thông báo bắt tay nằm ngoài phạm vi hoặc không phù hợp với các trường khác.

- **Cấu trúc TLS:**

Handshake Protocol: Đây là phần phức tạp nhất của TLS

- ✓ Giao thức này cho phép máy chủ và máy khách xác thực lẫn nhau và thương lượng một thuật toán mã hóa và MAC cũng như các khóa mật mã được sử dụng để bảo vệ dữ liệu được gửi trong bản ghi TLS.
- ✓ Giao thức bắt tay được sử dụng trước khi bất kỳ dữ liệu ứng dụng nào được truyền đi.
- ✓ Giao thức bắt tay bao gồm một loạt các thông báo được trao đổi bởi máy khách và máy chủ

- Cấu trúc TLS:

Handshake Protocol:

Mỗi tin nhắn có ba trường:

- Type (1 byte): Cho biết một trong 10 thông báo. Bảng 6.2 liệt kê các loại thông báo được xác định.
- Length (3 byte): Độ dài của tin nhắn tính bằng byte.
- Content (# 0 byte): Các tham số liên quan đến thông báo này (Bảng 6.2).

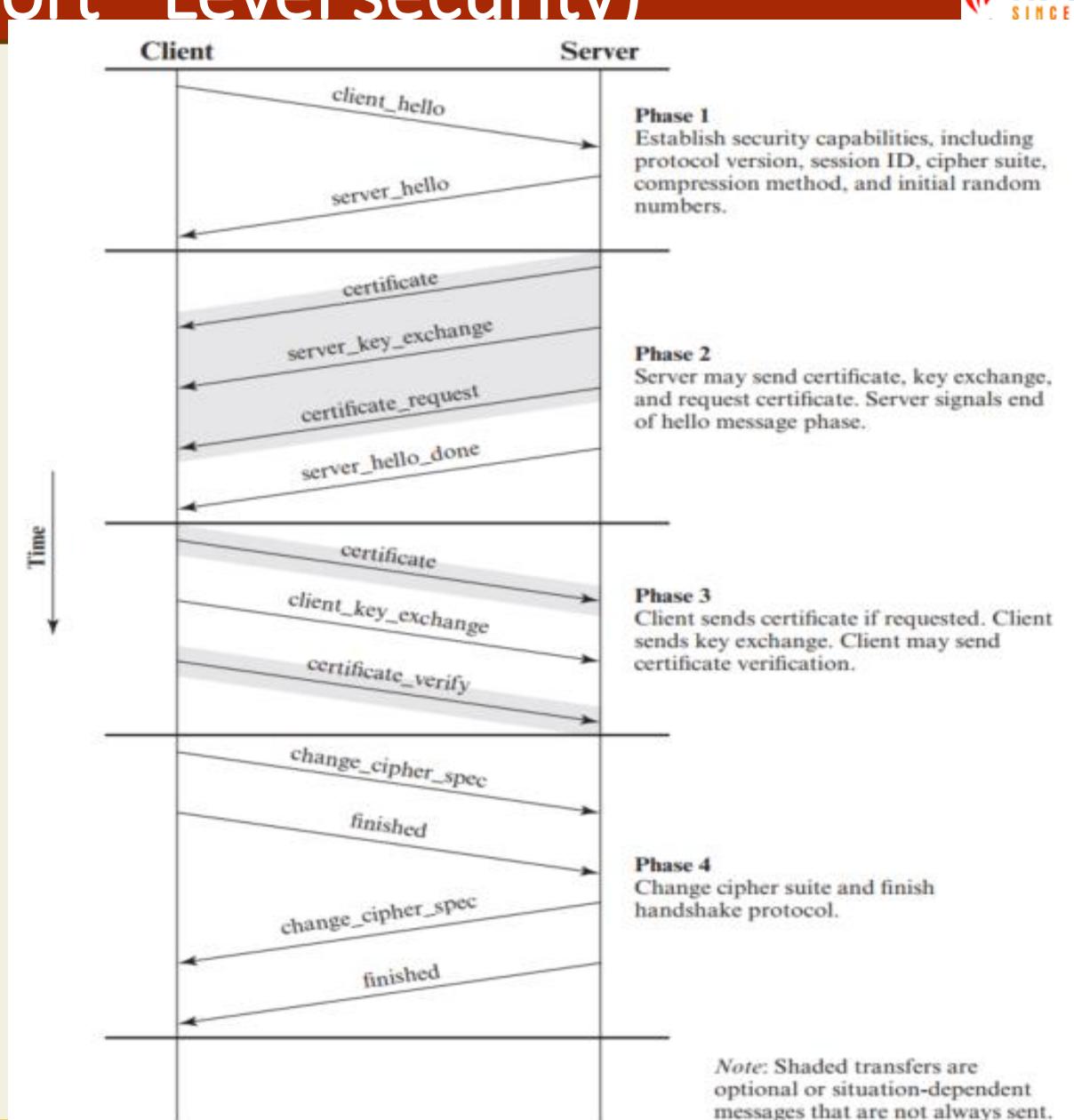
Table 6.2 TLS Handshake Protocol Message Types

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

- Cấu trúc TLS:

Handshake Protocol: 4 pha

Pha 1. Thiết lập khả năng bảo mật
 Giai đoạn 1 bắt đầu một kết nối logic và thiết lập các khả năng bảo mật sẽ được liên kết với nó. Quá trình trao đổi được bắt đầu bởi ứng dụng khách, ứng dụng này sẽ gửi message client_hello với các tham số: Version (TLS version), Random, Session ID



• Cấu trúc TLS:

Handshake Protocol: 4 pha

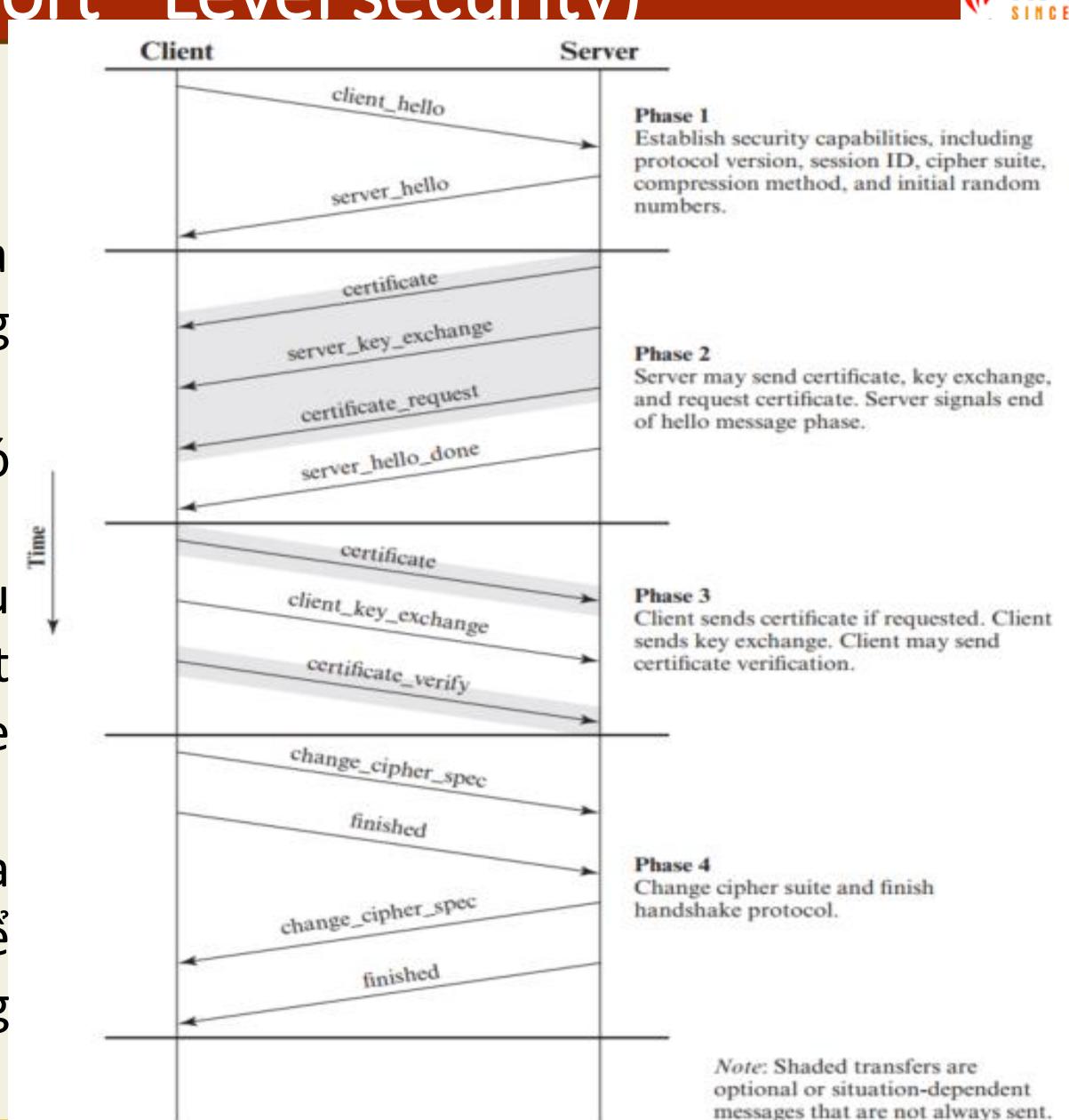
Pha 2. Xác thực máy chủ server và trao đổi khóa

Máy chủ bắt đầu pha này bằng cách gửi chứng chỉ của nó nếu nó cần được xác thực

Sau đó, một message `server_key_exchange` có thể được gửi nếu cần thiết.

Sau đó một máy chủ không ẩn danh có thể yêu cầu chứng chỉ từ client là `certificate_request` message – chứng chỉ này gồm `certificate_type` và `certificateAuthorities`

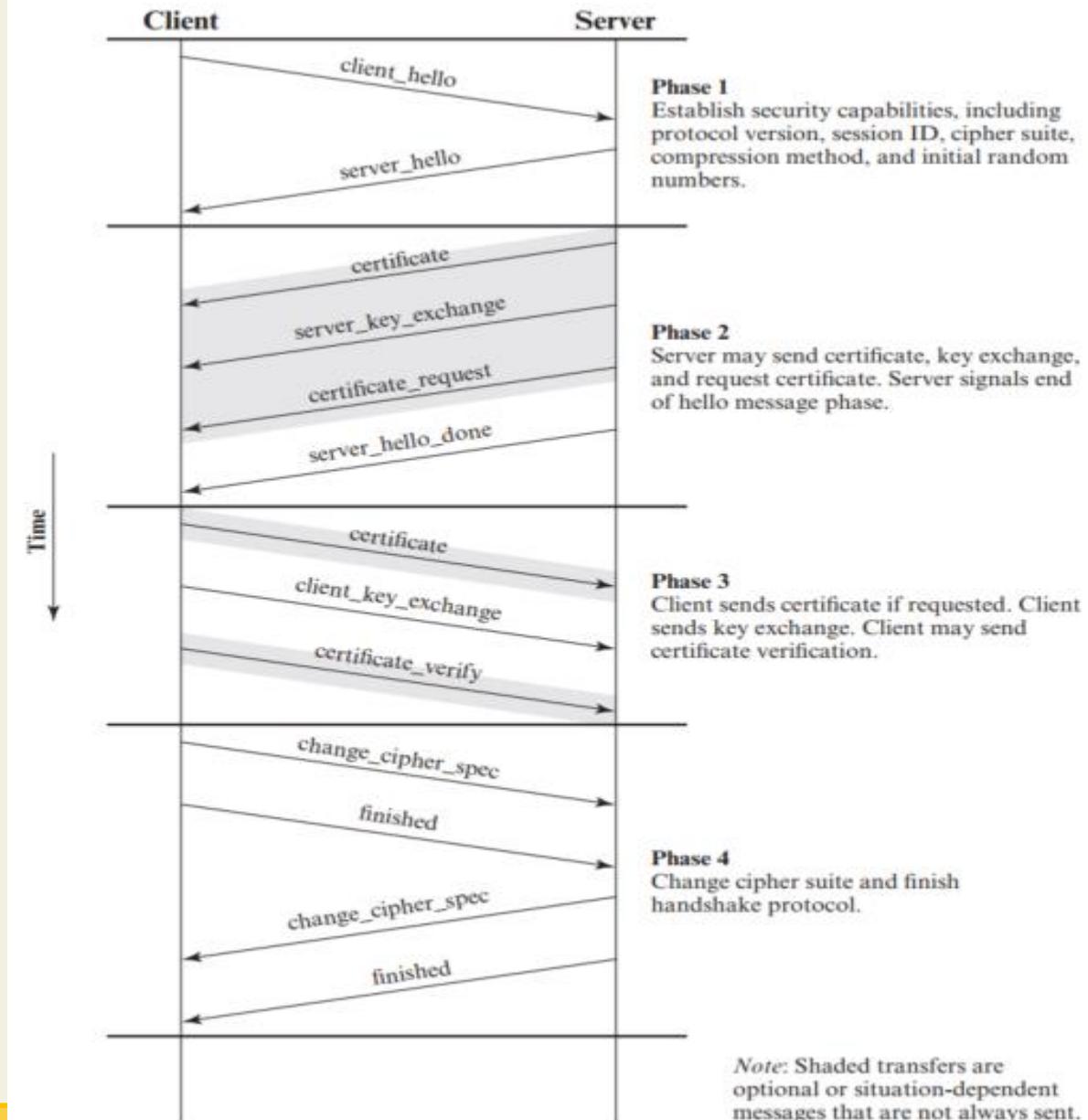
Message cuối cùng trong phase 2 là `server_done` message – được gửi từ server để cho biết đã kết thúc “server hello” và các thông báo liên quan.



- Cấu trúc TLS:

Handshake Protocol: 4 pha

Pha 3. Xác thực Client và trao đổi
khóa



- Cấu trúc TLS:

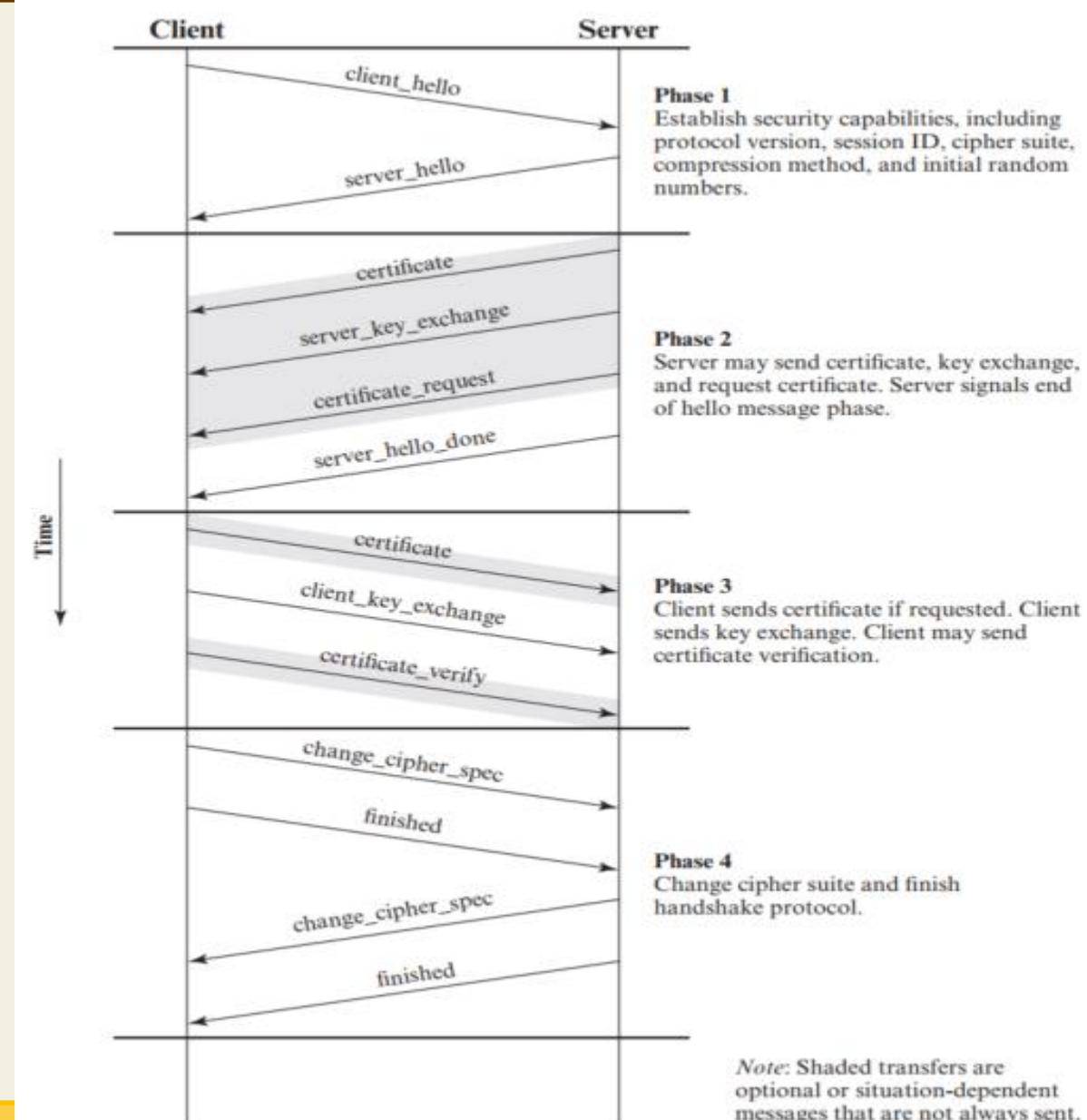
Handshake Protocol: 4 pha

Pha 4. Kết thúc – hoàn tất thiết lập kết nối an toàn.

Client gửi change_cipher_spec message

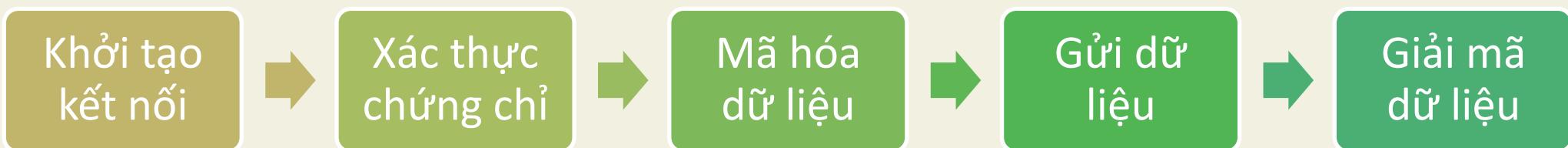
Client gửi finished message theo các thuật toán, khóa và bí mật mới.

Finished message xác minh rằng quá trình trao đổi khóa và xác thực thành công

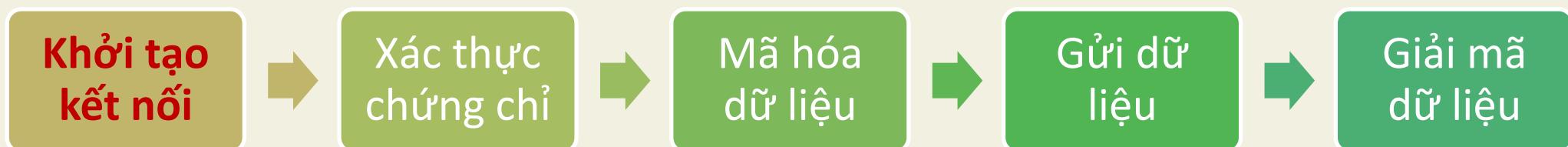


- **Cơ chế hoạt động của TLS:**

- TLS protocol hoạt động bằng cách sử dụng private key và cơ chế xác thực để bảo vệ dữ liệu truyền đi trên mạng
- Để hiểu rõ hơn cơ chế hoạt động của TLS, ta có thể phân tích quá trình bảo mật kết nối mạng theo các bước sau:



- Cơ chế hoạt động của TLS:



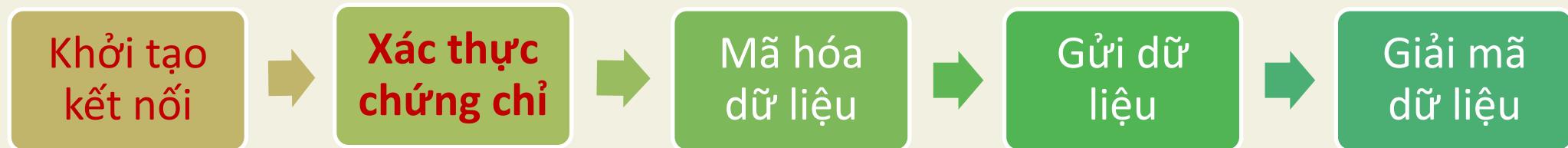
Trong quá trình **khởi tạo kết nối**, hai bên kết nối (ví dụ máy tính người dùng và *Web server*) sẽ trao đổi các thông tin cơ bản như phiên bản của TLS, các thuật toán *mã hóa* và các *chứng chỉ bảo mật*.

Web server: chịu trách nhiệm xử lý các yêu cầu truy cập từ các thiết bị khác (người dùng) và trả lại tài nguyên tương ứng. Có thể hiểu nó đóng vai trò quan trọng trong cung cấp nội dung cho người dùng trên Internet.

Thuật toán mã hóa: đối xứng và công khai

Chứng chỉ bảo mật: là các lối chứng chỉ bảo mật SSL (Secure Sockets layer) – là tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết được mã hóa giữa web server và trình duyệt.

- Cơ chế hoạt động của TLS:



Xác thực chứng chỉ: Sau khi 2 bên đã trao đổi các thông tin cơ bản, server sẽ gửi một chứng chỉ bảo mật đến máy tính của người dùng.

Máy tính người dùng sẽ kiểm tra chứng chỉ này bằng cách sử dụng các chứng chỉ của tổ chức xác thực đã được lưu trữ trên hệ thống

Nếu chứng chỉ được xác thực, kết nối sẽ tiếp tục, ngược lại sẽ ngắt kết nối

- Cơ chế hoạt động của TLS:



Mã hóa dữ liệu: Sau khi chứng chỉ đã được xác thực, hai bên sẽ sử dụng các private key để mã hóa dữ liệu trước khi gửi đi.

Những khóa này được tạo ra từ quá trình trao đổi thông tin cơ bản ban đầu và sẽ khác nhau giữa hai bên.

Khi dữ liệu được gửi đi, nó sẽ được mã hóa bằng các khóa này và chỉ người nhận dữ liệu mới có thể giải mã nó bằng các khóa bí mật của họ.

Nhờ có mã hóa dữ liệu, người dùng có thể yên tâm rằng dữ liệu của họ không bị truy cập bởi bất kì ai khác ngoài người nhận dữ liệu

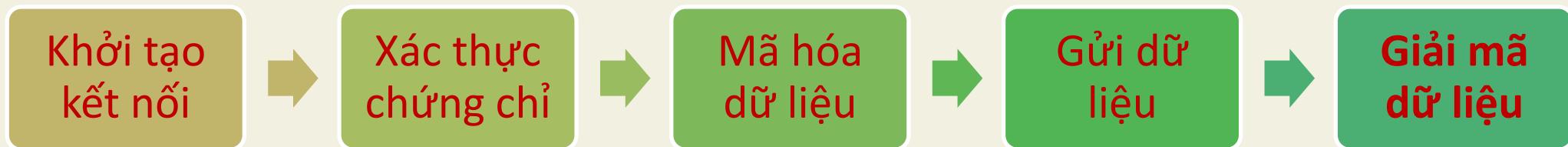
- Cơ chế hoạt động của TLS:



Gửi dữ liệu: Sau khi dữ liệu đã được mã hóa, nó có thể được gửi đi an toàn qua mạng.

Nếu có bất kỳ ai khác cố gắng truy cập dữ liệu này, họ sẽ không thể đọc được nội dung của nó vì nó đã được mã hóa bằng các khóa bí mật khác.

- Cơ chế hoạt động của TLS:



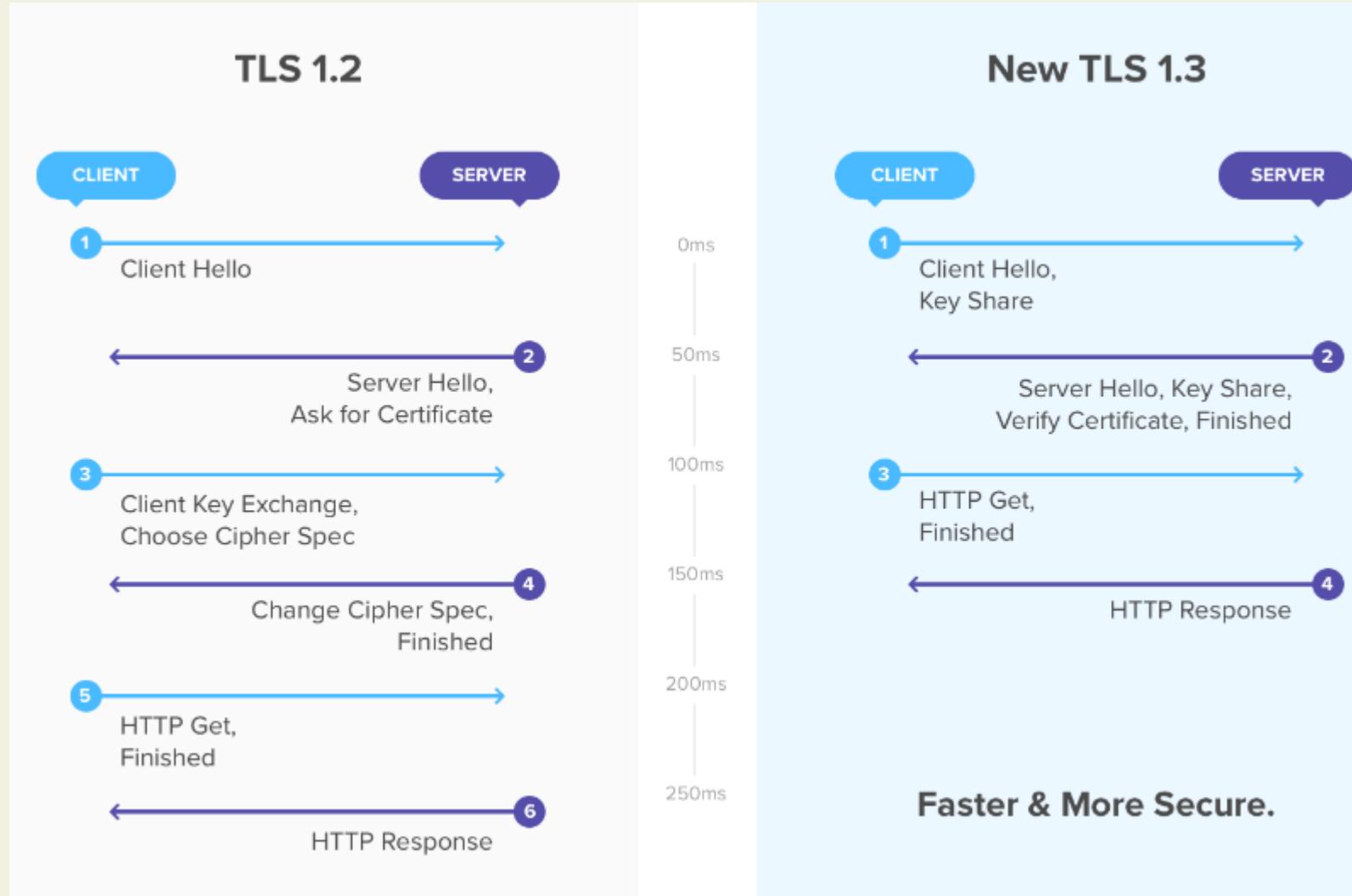
Giải mã dữ liệu: Khi dữ liệu đến tại người nhận, nó sẽ được giải mã bằng các khóa bí mật của người nhận để trở thành dữ liệu đọc được. Sau đó, người nhận có thể sử dụng dữ liệu này để thực hiện các thao tác cần thiết.

Như vậy, giao thức TLS hoạt động bằng cách sử dụng private key và cơ chế xác thực để bảo vệ dữ liệu trong quá trình truyền đi trên mạng. Nó giúp ngăn chặn các tấn công mạng và uy tín của doanh nghiệp trong mắt khách hàng và đối tác.

- Các phiên bản của TLS:

- 1.TLS 1.0:** Phiên bản đầu tiên của TLS, ra mắt vào năm 1999. TLS 1.0 đã được nâng cấp nhiều lần để khắc phục các lỗ hổng bảo mật, nhưng vẫn còn được sử dụng trên một số hệ thống cũ hơn.
- 2.TLS 1.1:** Phiên bản thứ hai của TLS, ra mắt vào năm 2006. TLS 1.1 đã khắc phục một số lỗ hổng bảo mật của TLS 1.0 và có sự cải tiến về hiệu năng.
- 3.TLS 1.2:** Phiên bản thứ ba của TLS, ra mắt vào năm 2008. TLS 1.2 là phiên bản được sử dụng rộng rãi hiện nay và đã khắc phục nhiều lỗ hổng bảo mật của TLS 1.0 và 1.1.
- 4.TLS 1.3:** Phiên bản mới nhất của TLS, ra mắt vào năm 2018. TLS 1.3 được coi là phiên bản bảo mật nhất và có sự cải tiến về hiệu năng so với các phiên bản trước.

- Giao thức TLS:



- **Ứng dụng TLS:**

- Truyền dữ liệu trên mạng:** Giao thức TLS được sử dụng để bảo vệ các kết nối mạng trong quá trình truyền thông dữ liệu giữa hai máy tính hoặc hệ thống mạng khác nhau.
- Truy cập các trang web an toàn:** Giao thức TLS được sử dụng để bảo vệ các kết nối truy cập trang web qua giao thức HTTPS (Hypertext Transfer Protocol Secure). Khi người dùng truy cập vào một trang web qua HTTPS, dữ liệu của họ sẽ được mã hóa.
- Gửi và nhận email:** Giao thức TLS cũng được sử dụng để bảo vệ các kết nối gửi và nhận email qua giao thức SMTP (Simple Mail Transfer Protocol) và IMAP (Internet Mail Access Protocol). Khi người dùng gửi hoặc nhận email qua một máy chủ email an toàn, dữ liệu được mã hóa bằng TLS để bảo vệ khỏi các tấn công mạng.
- Truy cập các dịch vụ trực tuyến:** Giao thức TLS cũng được sử dụng để bảo vệ các kết nối truy cập các dịch vụ trực tuyến, như ngân hàng trực tuyến, bảo hiểm trực tuyến và y tế trực tuyến.

Giới thiệu chung về HTTPS

- Hạn chế của HTTP:

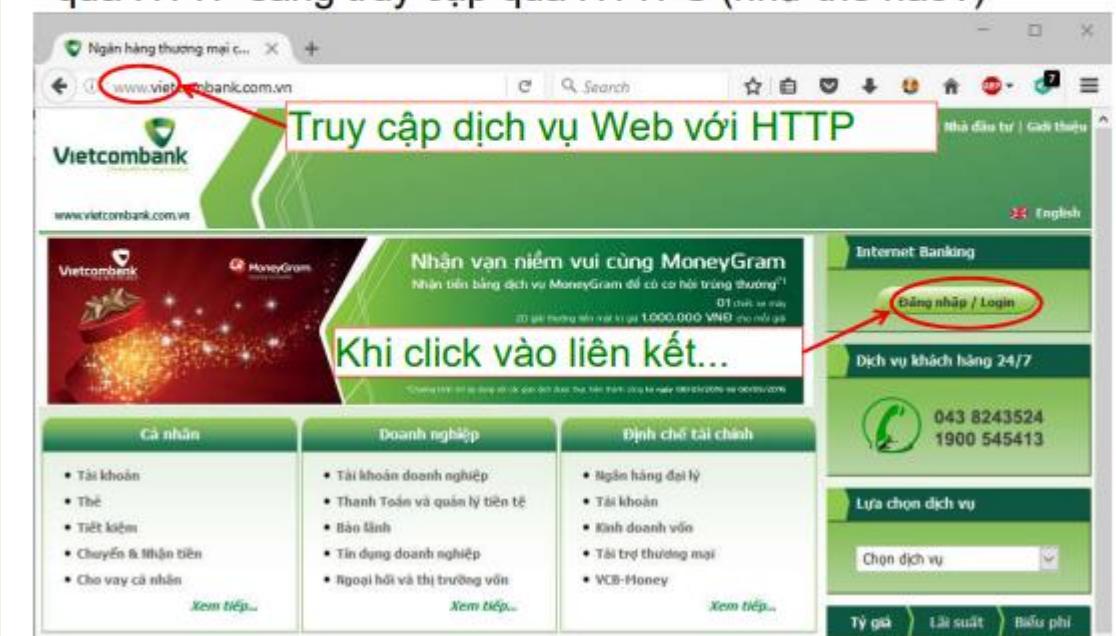
- Không có cơ chế để người dùng kiểm tra tính tin cậy của Web server → lỗ hổng để kẻ tấn công giả mạo dịch vụ hoặc chèn mã độc vào trang web HTML
- Không có cơ chế mã mật → lỗ hổng để kẻ tấn công nghe lén đánh cắp thông tin nhạy cảm

- Secure HTTP: Kết hợp HTTP và SSL/TLS:

- Xác thực
- Bảo mật

Tấn công vào HTTPS

- Tấn công sslstrip: lợi dụng lỗ hổng chuyển từ truy cập qua HTTP sang truy cập qua HTTPS (như thế nào?)



An ninh thư điện tử

- Sinh viên presentation

- Bài giảng cung cấp kiến thức tổng quan về an ninh IP
- Chính sách an ninh IP
- Authentication Header
- ESP: Encapsulating Security Payload
- Kết hợp các liên kết an ninh
- Sau khi học xong sinh viên giải thích được kiến trúc, mô hình hoạt động và thuật toán mã hóa của an ninh IP

- **Tổng quan về an ninh IP**

- Năm 1994, Hội đồng kiến trúc Internet (IAB: Internet Architecture Board) đã công bố một báo cáo có tên là “Security in the Internet Architecture” (RFC 1636)
- Báo cáo xác định các nhu cầu bảo mật cơ sở hạ tầng mạng khởi viêc giám sát và kiểm soát trái phép lưu lượng mạng và nhu cầu bảo mật lưu lượng từ người dùng cuối đến người dùng cuối bằng cơ chế **xác thực** và **mã hóa**.
- **IPSec được tích hợp sẵn trong IPv4 và IPv6 và được định nghĩa trong cùng các RFC.**

→ **IPsec: Internet Protocol Security – là một bộ giao thức mật mã bảo vệ lưu lượng dữ liệu qua mạng Internet Protocol**

- **Lý do cần IPSec:**

- Có những vấn đề an ninh cần giải quyết ở mức thấp hơn tầng ứng dụng: ví dụ chống tấn công giả mạo IP, phân tích, chặn bắt và xem trộm gói tin
- An ninh ở mức IP sẽ bảo đảm an ninh cho các ứng dụng kể cả ứng dụng chưa có tính năng an ninh

- **Các cơ chế an ninh IPSec:**

- Xác thực
- Bảo mật
- Quản lý khóa

- **Ứng dụng của IPSec:** IPsec cung cấp khả năng bảo mật thông tin liên lạc qua mạng LAN, qua các mạng WAN riêng và công cộng cũng như trên Internet

Cụ thể:

- Xây dựng mạng riêng ảo an toàn trên Internet: Tiết kiệm chi phí thiết lập và quản lý mạng riêng
- Truy nhập từ xa an toàn thông qua Internet: Tiết kiệm chi phí đi lại
- Thiết lập các kết nối mạng an toàn với các đối tác: Đảm bảo xác thực, bảo mật và cung cấp cơ chế trao đổi khóa
- Tăng cường an ninh thương mại điện tử: Hỗ trợ thêm cho các giao thức an ninh có sẵn của các ứng dụng Web và thương mại điện tử

Tính năng chính của IPsec cho phép nó hỗ trợ các ứng dụng đa dạng này là có thể mã hóa và/hoặc xác thực tất cả lưu lượng ở cấp độ IP. Do đó, tất cả các ứng dụng phân tán (bao gồm đăng nhập từ xa, máy khách/máy chủ, e-mail, truyền file, truy cập Web, v.v.) đều có thể được bảo mật

- Ví dụ minh họa về một mô hình IPSec-VPN sử dụng ESP
- VPN: (1) đảm bảo người dùng trái phép không xâm nhập được vào mạng VPN; (2) đảm bảo những kẻ nghe trộm không thể đọc được tin nhắn gửi qua VPN
- Như vậy VPN đảm bảo cả tính xác thực và mã hóa

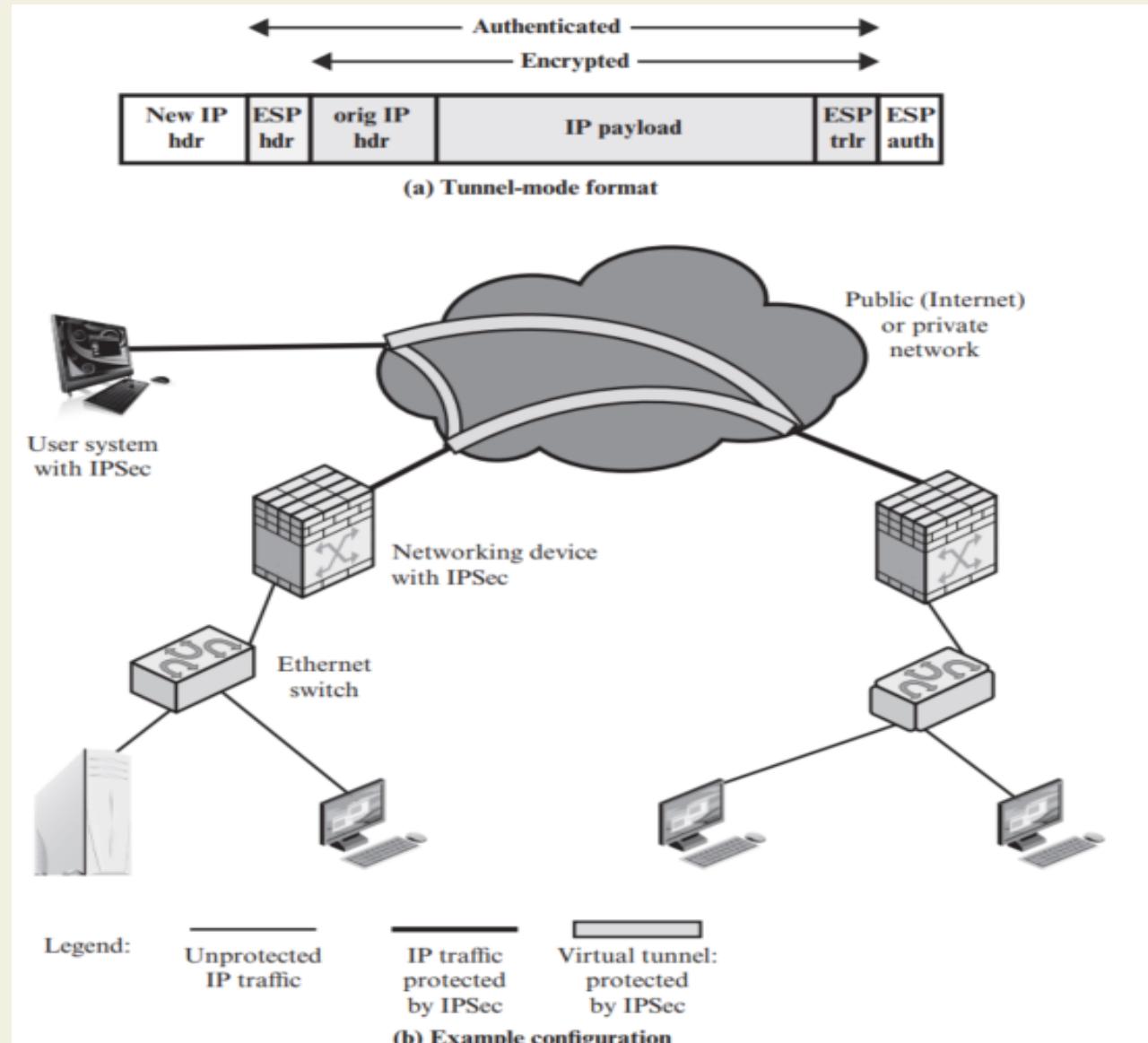


Figure 9.1 An IPSec VPN Scenario

Lợi ích của sử dụng IPSec:

- Tại tường lửa hoặc bộ định tuyến, IPSec đảm bảo an ninh cho mọi luồng thông tin vượt biên
- Tại tường lửa, IPSec ngăn chặn thâm nhập trái phép từ Internet vào
- IPSec nằm dưới tầng giao vận (TCP, UDP), do vậy trong suốt với các ứng dụng
- IPSec có thể trong suốt với người dùng cuối
- IPSec có thể áp dụng cho người dùng đơn lẻ
- IPSec bảo vệ an ninh kiến trúc định tuyến

Kiến trúc an ninh IP

- Đặc tả IPSec khá phức tạp
- Định nghĩa trong nhiều tài liệu:
 - Kiến trúc (RFC 4301), Authentication Header (RFC 4302), Encapsulating Security Payload (RFC 4303), Internet Key Exchange (RFC 4306)
 - AH không còn được sử dụng trong các ứng dụng mới
 - Các tài liệu mô tả các giải thuật mật mã:
 - Mã hóa, xác thực thông báo, hàm giả ngẫu nhiên, trao đổi khóa
 - Các tài liệu khác
 - Chính sách an ninh và cơ sở thông tin quản lý (MIB)
- Việc hỗ trợ IPSec là bắt buộc đối với IPv6, tùy chọn đối với IPv4

Các dịch vụ IPsec

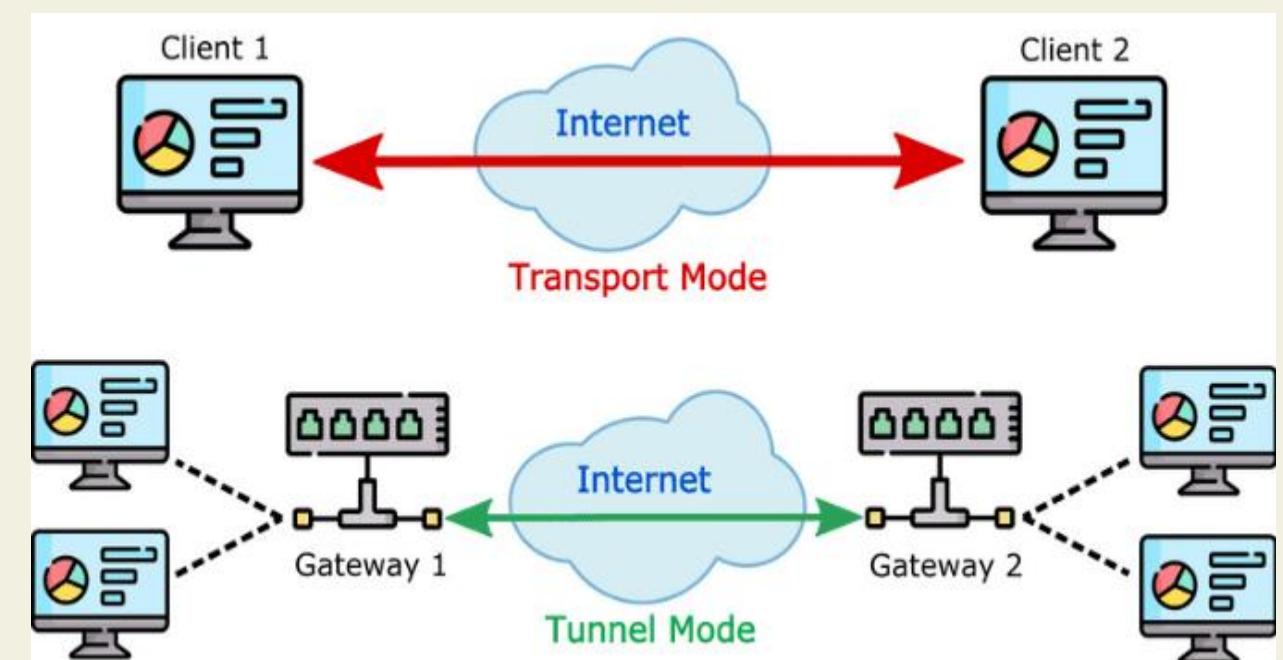
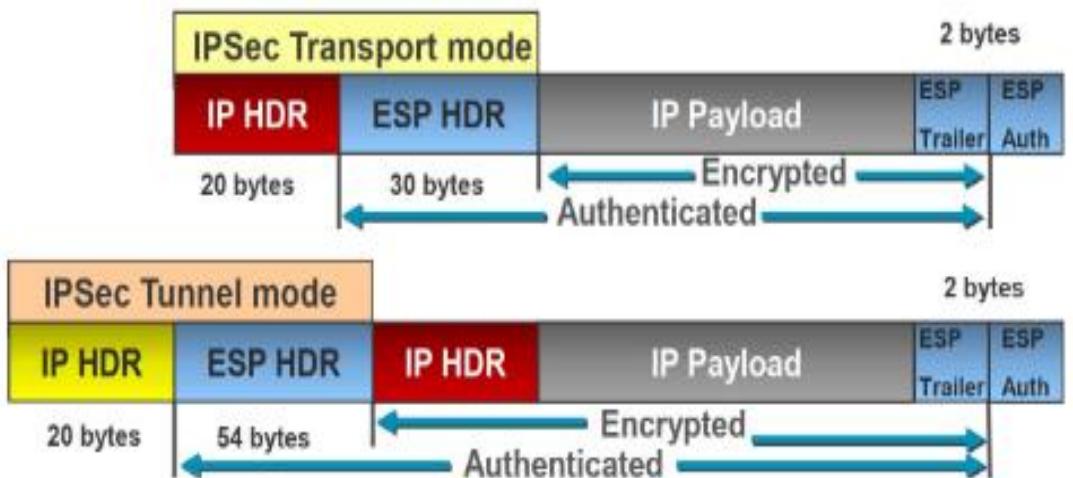
- RFC 4301 liệt kê các dịch vụ sau:
 - Kiểm soát truy cập
 - Tính toàn vẹn phi kết nối
 - Xác thực nguồn gốc dữ liệu
 - Từ chối các gói phát lại (một dạng toàn vẹn chuỗi một phần)
 - Bảo mật (mã hóa)
 - Bảo mật lưu lượng hạn chế

Các giao thức chính của IPSec:

- Giao thức AH – Authentication Header hay Tiêu đề xác thực: là một giao thức xác thực được chỉ định bởi tiêu đề của giao thức. Mới bảo đảm được tính **xác thực**.
- Giao thức đóng gói tải trọng bảo mật ESP - Encapsulation Secure Payload : một giao thức mã hóa/xác thực kết hợp có nghĩa là bảo đảm cả tính **xác thực** và **mã hóa**
- Như vậy: AH đảm bảo tính xác thực và toàn vẹn gói tin Ip, gói tin không được mã hóa. Nếu cần thêm tính bí mật thì sử dụng ESP: ESP vừa bảo đảm tính toàn vẹn và bí mật

Transport and Tunnel Modes

- Cả AH và ESP đều hỗ trợ hai chế độ sử dụng: chế độ vận chuyển và đường hầm (transport mode và tunnel mode). Tuy nhiên, hoạt động của hai chế độ này được hiểu rõ nhất trong bối cảnh mô tả ESP.
- Transport mode cung cấp cơ chế bảo vệ cho dữ liệu của các lớp cao hơn (TCP, UDP hoặc ICMP) trong khi đó Tunnel Mode sẽ bảo vệ toàn bộ gói dữ liệu.



Transport and Tunnel Modes

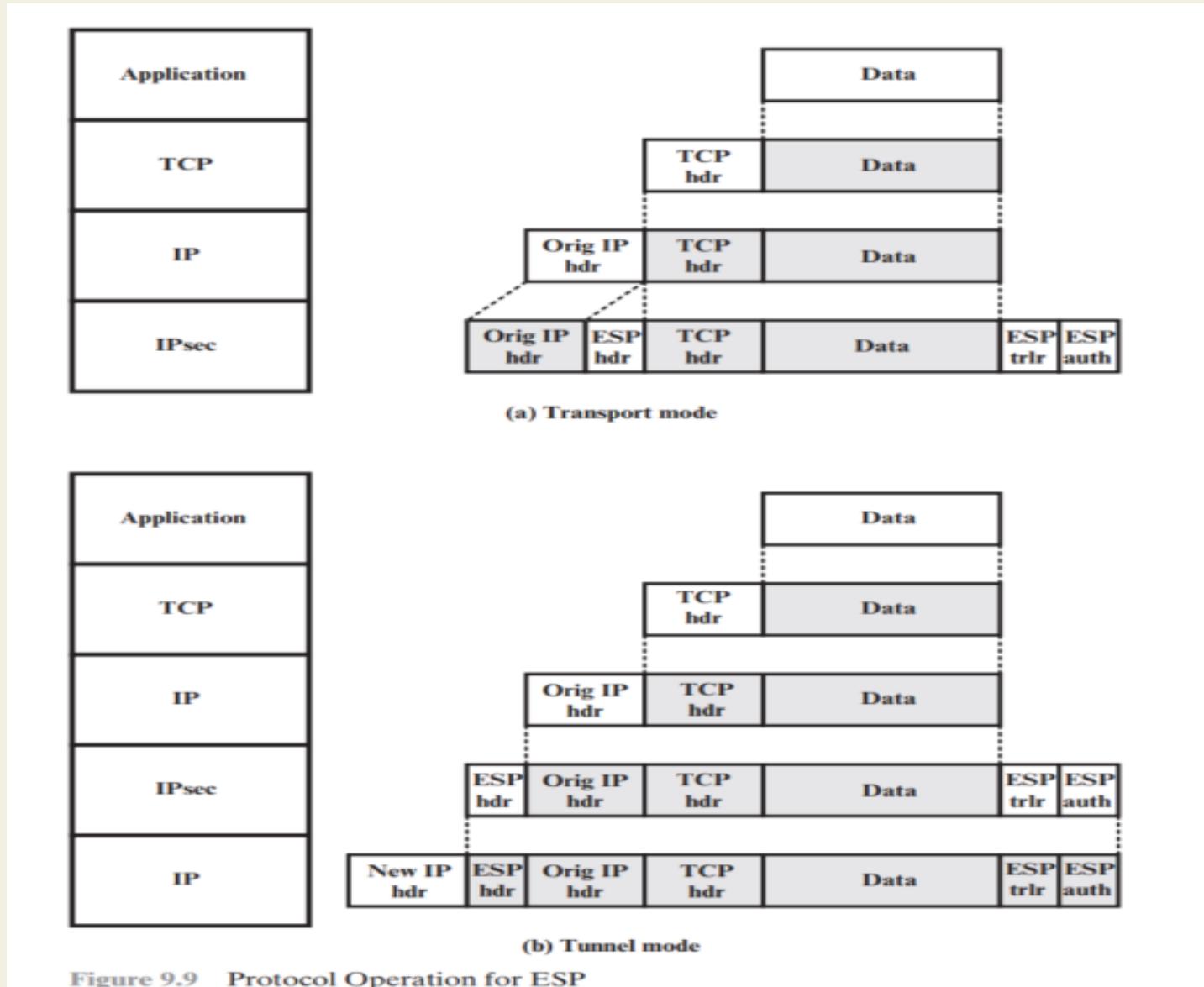
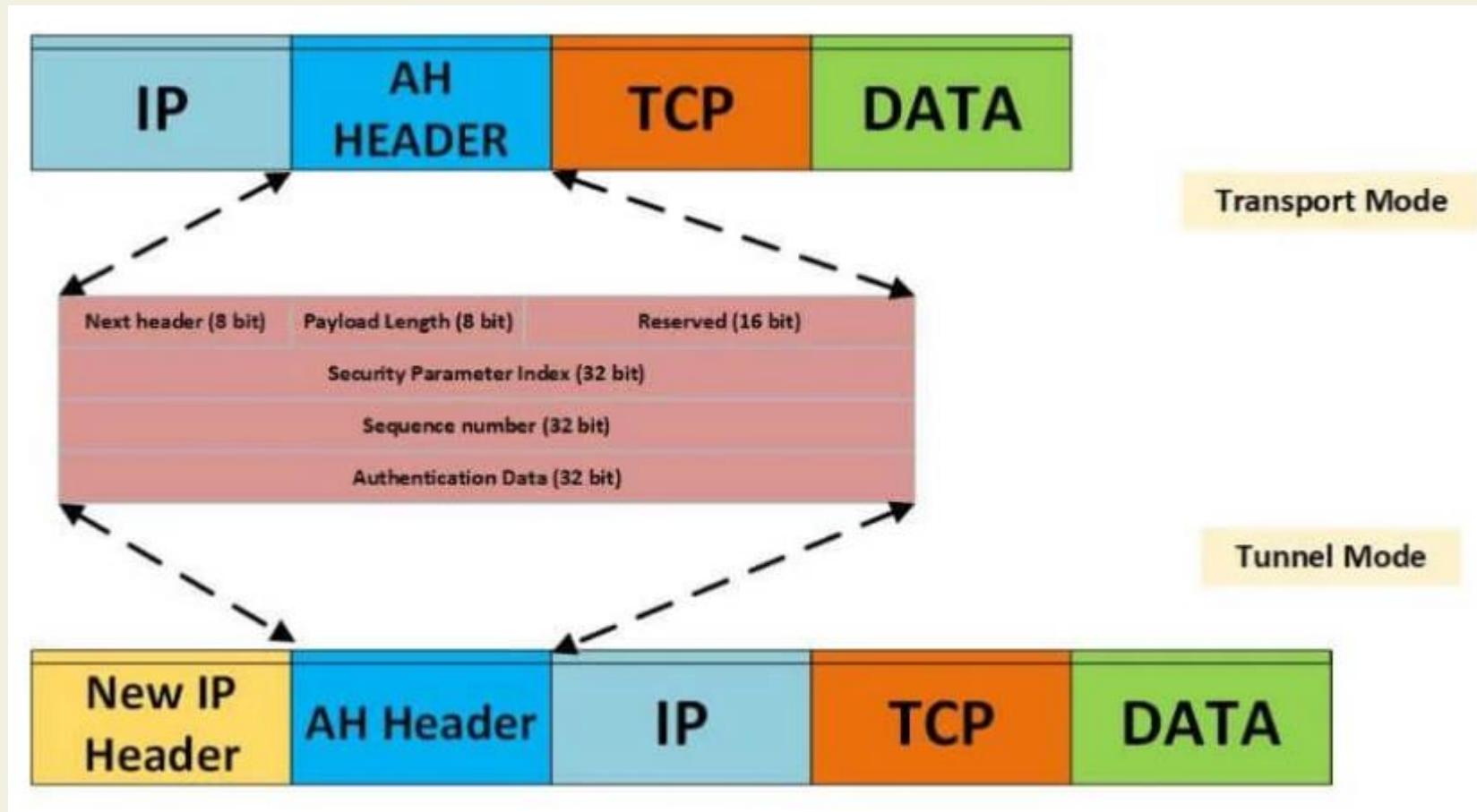


Figure 9.9 Protocol Operation for ESP

Giao thức xác thực AH: AH cho phép xác thực người dùng, xác thực ứng dụng và thực hiện các cơ chế lọc gói tương ứng. Ngoài ra AH còn có khả năng hạn chế các tấn công giả danh (spoofing) và tấn công phát lại (replay).
Cấu trúc gói:



Giao thức xác thực AH

- **Cơ chế chống phát lại:** Cơ chế này cho phép ngăn chặn các tấn công dạng phát lại (replay), tức là bắt gói, lưu trữ rồi phát lại.
 - Trường số thứ tự (Sequence Number) trong tiêu đề AH được dùng để đánh dấu thứ tự các gói được gửi đi trên một SA.
 - Ban đầu, giá trị này được khởi tạo bằng 0 và tăng dần sau mỗi gói được gửi. Để đảm bảo không có gói lặp lại, khi số thứ tự đạt giá trị cực đại ($2^{32} - 1$), nó sẽ không được quay lại giá trị 0, mà thay vào đó, một SA với khoá mới được thiết lập để tiếp tục việc truyền dữ liệu. Điều này đảm bảo trên cùng một SA không bao giờ có hai gói dữ liệu có số thứ tự trùng nhau.
 - Ở phía nhận, quá trình xử lý các gói nhận được thực hiện phức tạp hơn nhằm phát hiện các gói lặp nhau. Do IP không thiết lập kết nối và không đảm bảo truyền tin cậy, do đó việc sai thứ tự, lặp, hoặc mất gói là điều có thể xảy ra.

Giao thức xác thực AH

- **Xác thực thông tin:** Mã xác thực (trường Authentication Data) được tạo ra dùng một trong hai cách sau:
 - HMAC-MD5-96: dùng phương pháp HMAC, hàm băm là MD5, cắt lấy 96 bit đầu tiên.
 - HMAC-SHA-1-96: dùng phương pháp HMAC, hàm băm là SHA-1, cắt lấy 96 bit đầu tiên.

Thuật toán MAC được áp dụng trên các phần thông tin sau đây:

- Các trường không bị thay đổi trong tiêu đề gói IP khi được chuyển tiếp trên mạng hoặc có thể dự đoán được tại đầu cuối của SA. Những trường còn lại trong tiêu đề gói IP được thay bằng các bit 0 khi tính toán.
- Các trường trong tiêu đề AH, ngoại trừ trường Authentication Data. Trường này được thay bằng các bit 0 khi tính.
- Toàn bộ dữ liệu của lớp trên (tức phần payload của gói IP).

Giao thức xác thực AH

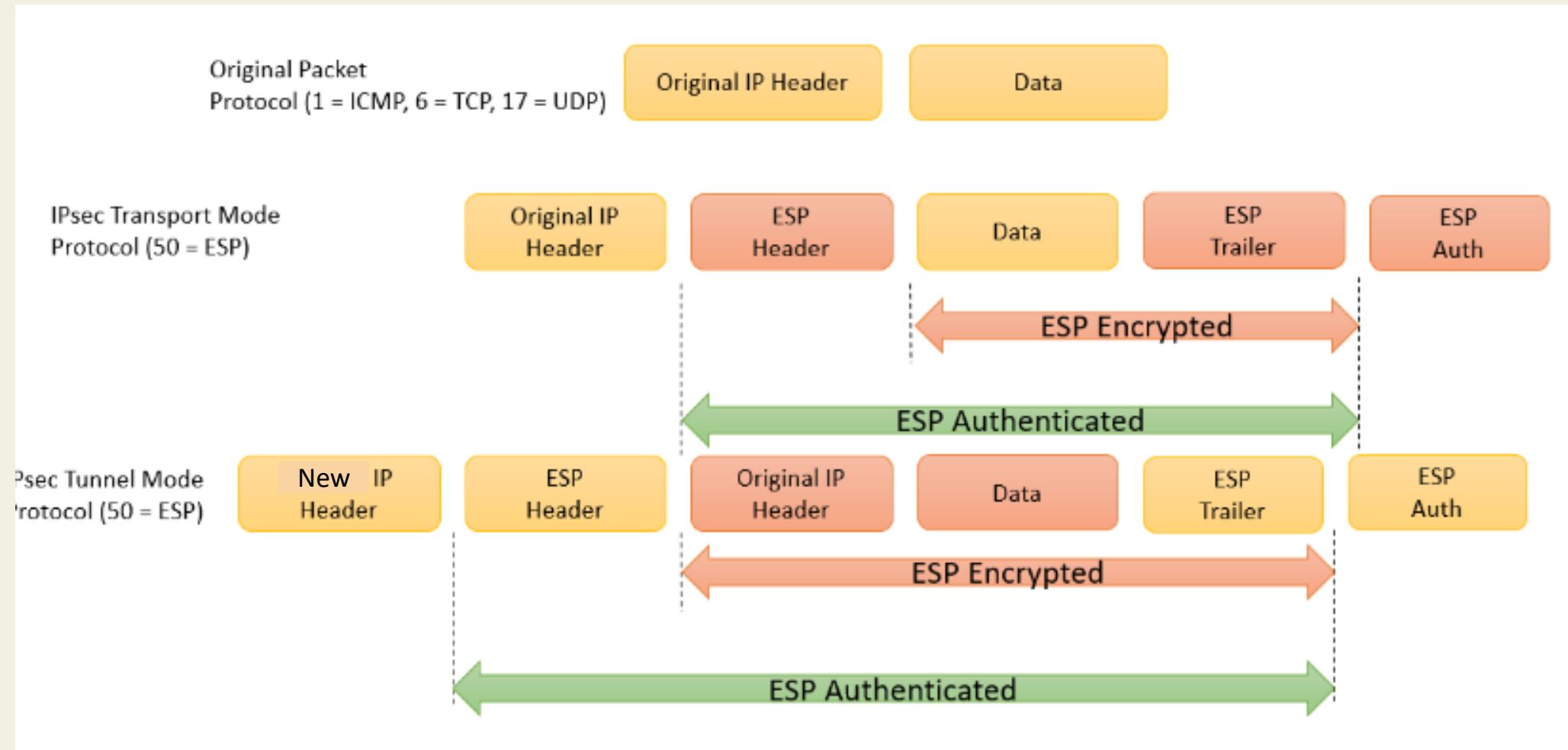
Cơ chế xác thực:

- Xác thực từ đầu cuối đến đầu cuối (End-to-End Authentication): là trường hợp xác thực trực tiếp giữa hai hệ thống đầu cuối (giữa máy chủ với trạm làm việc hoặc giữa hai trạm làm việc), việc xác thực này có thể diễn ra trên cùng mạng nội bộ hoặc giữa hai mạng khác nhau, chỉ cần hai đầu cuối biết được khoá bí mật của nhau. Trường hợp này sử dụng chế độ vận chuyển (Transport Mode) của AH.
- Xác thực từ đầu cuối đến trung gian (End-to-Intermediate Authentication): là trường hợp xác thực giữa hệ thống đầu cuối với một thiết bị trung gian (router hoặc firewall). Trường hợp này sử dụng chế độ đường hầm (Tunnel Mode) của AH.

Giao thức đóng gói ESP - Encapsulating Security Payload là một lựa chọn khác để thực thi IPSec bên cạnh giao thức xác thực thông tin AH.

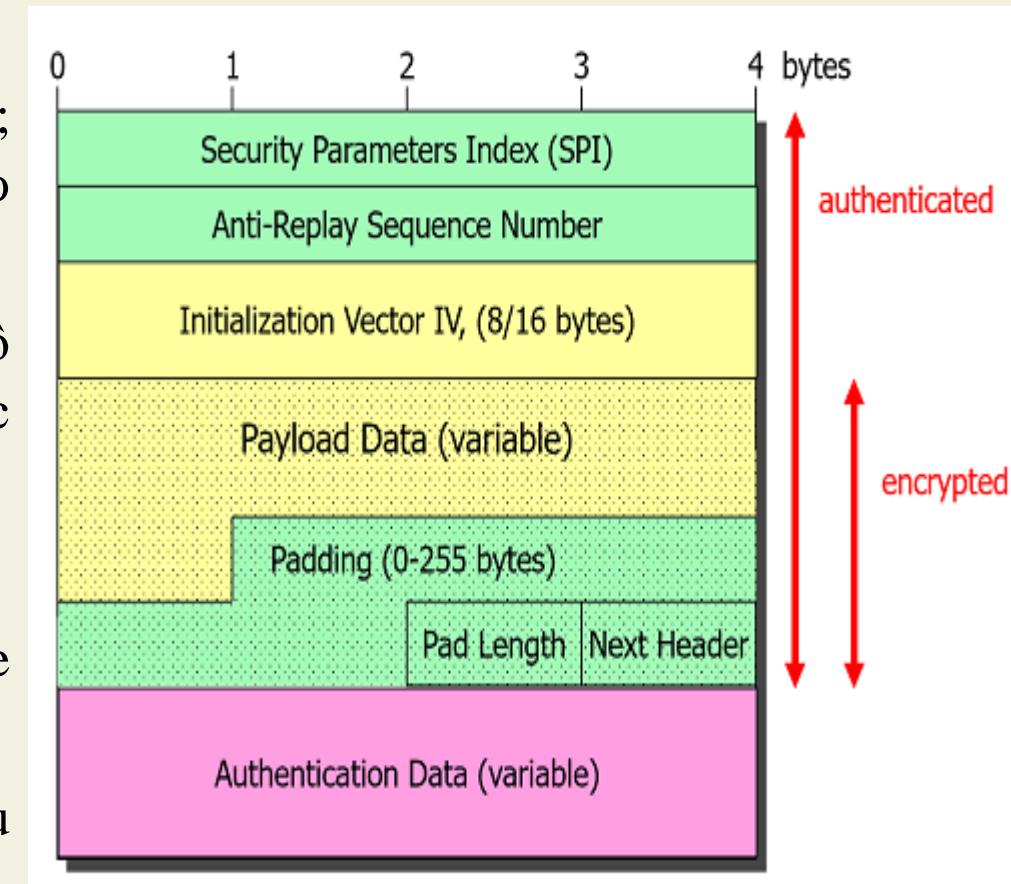
- Chức năng chính của ESP là cung cấp tính bảo mật cho dữ liệu truyền trên mạng IP bằng các kỹ thuật mật mã.
- Tuy nhiên ESP cũng còn một tuỳ chọn khác là cung cấp cả dịch vụ bảo đảm tính toàn vẹn của dữ liệu thông qua cơ chế xác thực.
- Như vậy khi sử dụng ESP, người dùng có thể chọn hoặc không chọn chức năng xác thực, còn chức năng mã hoá là chức năng mặc định của ESP.

Giao thức đóng gói ESP - Encapsulating Security Payload



Giao thức đóng gói ESP - Encapsulating Security Payload: Kiến trúc gói ESP

- Security parameter index - Chỉ mục tham số bảo mật (32 bit): Xác định liên kết bảo mật.
- Sequence number- Số thứ tự (32 bit): Giá trị bộ đếm tăng dần đều; điều này cung cấp chức năng chống phát lại, như đã thảo luận cho AH.
- Dữ liệu tải trọng - Payload data (variable): Đây là phân đoạn cấp độ truyền tải (chế độ truyền tải) hoặc gói IP (chế độ đường hầm) được bảo vệ bằng mã hóa.
- Đệm - Padding (0–255 byte): được sử dụng để mở rộng bản rõ
- Độ dài vùng đệm - Buffer length (8 bit): Cho biết số lượng byte vùng đệm ngay trước trường này.
- Next header (8 bit): Xác định loại dữ liệu chứa trong trường dữ liệu tải trọng bằng cách xác định tiêu đề đầu tiên trong tải trọng đó
- Giá trị kiểm tra tính toàn vẹn ICV- Integrity Check Value (variable)



Giao thức đóng gói ESP

Nguyên tắc hoạt động:

- Về nguyên tắc hoạt động thì ESP sử dụng mật mã đối xứng để cung cấp sự mật hoá dữ liệu cho các gói tin IPSec.
- Cho nên, để kết nối của cả hai đầu cuối đều được bảo vệ bởi mã hoá ESP thì hai bên phải sử dụng key giống nhau mới mã hoá và giải mã được gói tin.
- Khi một đầu cuối mã hoá dữ liệu, nó sẽ chia dữ liệu thành các khối (block) nhỏ, và sau đó thực hiện thao tác mã hoá nhiều lần sử dụng các block dữ liệu và khóa (key).
- Khi một đầu cuối khác nhận được dữ liệu mã hoá, nó thực hiện giải mã sử dụng key giống nhau và quá trình thực hiện tương tự, nhưng trong bước này ngược với thao tác mã hoá.

Quản lý khóa: Để áp dụng hai mào đầu AH và ESP yêu cầu các bên tham gia phải thỏa thuận một khóa chung để sử dụng trong việc kiểm tra an toàn thông tin.

- Quản lý khóa thủ công: IPv6 yêu cầu tất cả các thao tác đều có thể cho phép thiết lập thủ công khóa bí mật. Công nghệ cấu hình bằng tay được cho phép trong IPSec chuẩn và có thể được chấp nhận để cấu hình một hay hai gateway nhưng việc gõ key bằng tay không thích hợp trong một số trường hợp số lượng các gateway nhiều và cũng gây ra các vấn đề không an toàn trong quá trình tạo khóa.
- Quản lý khóa tự động: Internet Key Exchange (IKE) cung cấp key một cách tự động, quản lý SA hai chiều, tạo key và quản lý key. IKE thường thuyết trong hai giai đoạn.
 - Giai đoạn 1: thương thuyết bảo mật, kênh chứng thực mà dựa trên đó hệ thống có thể thương thuyết nhiều giao thức khác. Chúng đồng ý thuật toán mã hoá, thuật toán hash, phương pháp chứng thực và nhóm Diffie-Hellman để trao đổi key và thông tin.
 - Giai đoạn 2: xác định dịch vụ được sử dụng bởi IPSec. Chúng đồng ý giao thức IPSec, thuật toán hash, và thuật toán mã hoá. Một SA được tạo ra cho inbound và outbound của mỗi giao thức được sử dụng.

IPSec – VPN

IP sec có 3 mục tiêu chính:

- Xác thực thiết bị đầu xa
- Mã hóa
- Đảm bảo tính toàn vẹn

Do đó VPN - Virtual private network là một kết nối được mã hóa giữa hai hoặc nhiều máy tính. Kết nối VPN diễn ra qua các public network, nhưng dữ liệu trao đổi qua VPN vẫn là riêng tư vì nó được mã hóa.

Xây dựng VPN qua 2 giai đoạn: phase 1 (mục tiêu xây dựng đường hầm an toàn) từ đó xây dựng đường hầm phase 2 – chứa 2 đường hầm con để truyền dữ liệu giữa 2 mạng LAN

Phase 1: 2 router sẽ trao đổi với nhau một proposal:

- Xác thực: Đơn giản nhất là thống nhất mật khẩu giữa 2 router
- Mã hóa: sử dụng mã hóa nào?
- Khóa: phân phối khóa dùng DH
- Mã hash: đảm bảo tính toàn vẹn

- ESP hay AH được sử dụng để bảo vệ gói tin trong đường hầm phase 2 và chỉ được chọn 1 trong 2.
- AH đảm bảo tính xác thực và toàn vẹn gói tin Ip, gói tin không được mã hóa.
- Nếu cần thêm tính bí mật thì sử dụng ESP: ESP vừa bảo đảm tính toàn vẹn và bí mật.
- Mode transport: kết hợp với nhiều đường hầm khác
- Mode tunnel: thường được sử dụng, giữa máy tính laptop và mạng LAN,... hầu hết trường hợp sử dụng mode tunnel

An ninh mạng không dây

NỘI DUNG CHÍNH

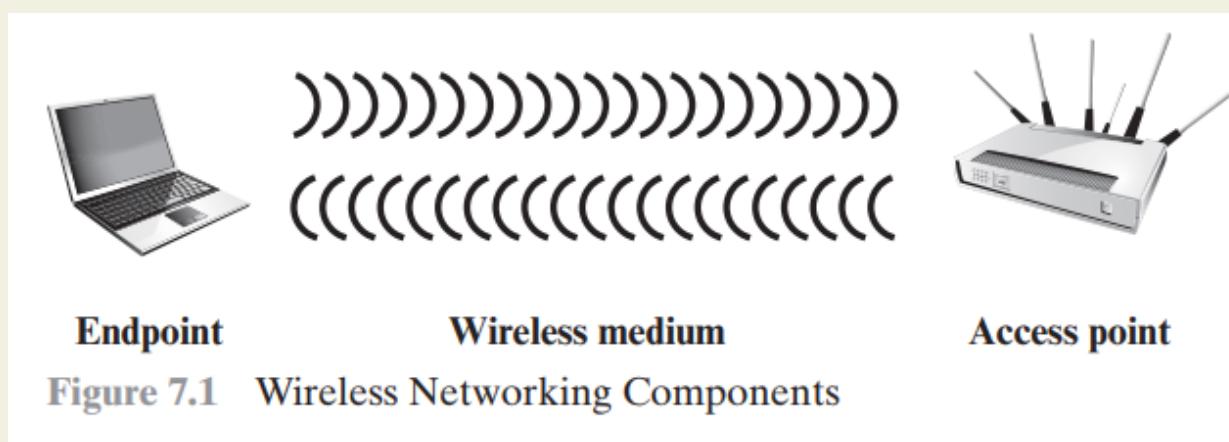
- Giới thiệu chung về an ninh mạng không dây
- An ninh thiết bị di động
- Công nghệ Wireless LAN
- An ninh mạng không dây WLAN theo chuẩn IEEE 802.11i



1. Giới thiệu chung về an ninh mạng không dây

Các yếu tố làm tăng nguy cơ mất an toàn đối với mạng không dây:

- **Kênh truyền tin - channel:** Mạng không dây thường liên quan đến truyền thông quảng bá, dễ bị nghe lén và gây nhiễu hơn nhiều so với mạng có dây.
- **Tính di động - mobility:** Các thiết bị không dây, thường dễ mang theo và di động hơn nhiều so với các thiết bị có dây
- **Tài nguyên - resources:** Một số thiết bị không dây có hệ điều hành phức tạp nhưng bộ nhớ hạn chế và tài nguyên xử lý để chống lại các mối đe dọa, bao gồm từ chối dịch vụ và phần mềm độc hại.
- **Khả năng truy cập – access ability:** Một số thiết bị không dây, chẳng hạn như cảm biến và rô-bốt, có thể không được giám sát ở các địa điểm xa xôi và/hoặc ở vị trí của kẻ tấn công.



1. Giới thiệu chung về an ninh mạng không dây

Các nguy cơ mất an toàn với mạng không dây:

- **Kết nối chồng chéo ngẫu nhiên:** Mạng LAN không dây hoặc điểm truy cập không dây của công ty với mạng LAN có dây ở gần nhau (ví dụ: trong cùng tòa nhà hoặc tòa nhà lân cận) có thể tạo phạm vi truyền chồng chéo → vô tình kết nối → lộ tài nguyên
- **Liên kết độc hại:** một thiết bị không dây được cấu hình như một điểm truy cập hợp pháp, cho phép người điều khiển đánh cắp mật khẩu từ những người dùng hợp pháp và sau đó xâm nhập mạng có dây.
- **Mạng ad hoc:** Đây là các mạng ngang hàng giữa các máy tính không dây không có điểm truy cập giữa chúng. Các mạng như vậy có thể gây ra mối đe dọa bảo mật do thiếu điểm kiểm soát trung tâm.
- **Mạng phi truyền thống:** Các mạng và liên kết phi truyền thống, chẳng hạn như thiết bị Bluetooth mạng cá nhân, đầu đọc mã vạch và PDA cầm tay, gây ra rủi ro bảo mật về cả nghe lén và giả mạo.

Giới thiệu chung về an ninh mạng không dây

Các nguy cơ mất an toàn với mạng không dây:

- **Trộm danh tính (giả mạo MAC):** Điều này xảy ra khi kẻ tấn công có thể nghe trộm lưu lượng mạng và xác định địa chỉ MAC của máy tính có đặc quyền mạng.
- **Tấn công trung gian:** cuộc tấn công này liên quan đến việc thuyết phục người dùng và điểm truy cập tin rằng họ đang nói chuyện với nhau trong khi thực tế giao tiếp đang đi qua một thiết bị tấn công trung gian.
- **Tù chối dịch vụ (DoS):** tấn công DoS xảy ra khi kẻ tấn công liên tục tấn công điểm truy cập không dây hoặc một số cổng không dây có thể truy cập khác bằng nhiều giao thức khác nhau thông báo được thiết kế để tiêu thụ tài nguyên hệ thống.
- **Chèn mạng:** Một cuộc tấn công chèn mạng nhắm vào các điểm truy cập không dây tiếp xúc với lưu lượng mạng chưa được lọc, chẳng hạn như thông báo giao thức định tuyến hoặc thông báo quản lý mạng. Một ví dụ về cuộc tấn công như vậy là một cuộc tấn công trong đó các lệnh cấu hình lại không có thật được sử dụng để tác động đến các bộ định tuyến và chuyển mạch nhằm làm giảm hiệu suất mạng.

Các biện pháp bảo mật không dây

- **Bảo mật đường truyền không dây:** Các mối đe dọa chính đối với đường truyền không dây là nghe trộm, thay đổi hoặc chèn thông báo và gián đoạn

■ *Kỹ thuật che giấu tín hiệu:* Các tổ chức có thể thực hiện một số biện pháp để khiến kẻ tấn công khó xác định vị trí các điểm truy cập không dây của họ hơn, bao gồm tắt phát sóng định danh bộ dịch vụ (SSID: service set identifier) bởi các điểm truy cập không dây; gán tên khó hiểu cho SSID; giảm cường độ tín hiệu xuống mức thấp nhất mà vẫn cung cấp vùng phủ sóng cần thiết; và định vị các điểm truy cập không dây ở bên trong tòa nhà, cách xa cửa sổ và tường bên ngoài.

■ *Mã hóa:* Mã hóa tất cả quá trình truyền không dây có hiệu quả chống nghe lén trong phạm vi các khóa mã hóa được bảo mật. Việc sử dụng các giao thức mã hóa và xác thực là phương pháp tiêu chuẩn để chống lại các nỗ lực thay đổi hoặc chèn đường truyền.

Các biện pháp bảo mật không dây

- **Bảo mật các điểm truy cập không dây:** Mối đe dọa chính liên quan đến các điểm truy cập không dây là truy cập trái phép vào mạng.
 - Phương pháp chính để ngăn chặn truy cập như vậy là tiêu chuẩn IEEE 802.1X cho kiểm soát truy cập mạng dựa trên cổng.
 - Tiêu chuẩn cung cấp cơ chế xác thực cho các thiết bị muốn kết nối với mạng LAN hoặc mạng không dây.
 - Việc sử dụng 802.1X có thể ngăn các điểm truy cập lừa đảo và các thiết bị trái phép khác trở thành cửa hậu không an toàn.

Các biện pháp bảo mật không dây

• *Bảo mật mạng không dây:*

- 1. Sử dụng mã hóa. Bộ định tuyến không dây thường được trang bị cơ chế mã hóa tích hợp cho lưu lượng từ bộ định tuyến đến bộ định tuyến.
- 2. Sử dụng phần mềm chống vi-rút và phần mềm gián điệp và tường lửa. Các cơ sở này nên được kích hoạt trên tất cả các điểm cuối mạng không dây.
- 3. Tắt phát sóng định danh. Bộ định tuyến không dây thường được định cấu hình để phát tín hiệu nhận dạng sao cho bất kỳ thiết bị nào trong phạm vi có thể biết được sự tồn tại của bộ định tuyến. Nếu một mạng được cấu hình sao cho các thiết bị được ủy quyền biết danh tính của các bộ định tuyến, khả năng này có thể bị vô hiệu hóa để ngăn chặn những kẻ tấn công.
- 4. Thay đổi mã định danh trên bộ định tuyến của bạn từ mặc định. Một lần nữa, biện pháp này ngăn chặn những kẻ tấn công sẽ cố gắng giành quyền truy cập vào mạng không dây bằng cách sử dụng mã định danh bộ định tuyến mặc định.
- 5. Thay đổi mật khẩu cài sẵn của bộ định tuyến để quản trị.
- 6. Chỉ cho phép các máy tính cụ thể truy cập mạng không dây. Một bộ định tuyến có thể được cấu hình để chỉ giao tiếp với các địa chỉ MAC đã được phê duyệt. Tất nhiên, địa chỉ MAC có thể bị giả mạo, vì vậy đây chỉ là một phần của chiến lược bảo mật.

2. Bảo mật thiết bị di động

Một số vấn đề về mạng của một tổ chức:

- Việc sử dụng các thiết bị mới ngày càng tăng: Các tổ chức đang có sự gia tăng đáng kể về mức độ sử dụng thiết bị di động của nhân viên.
- Các ứng dụng dựa trên đám mây: Các ứng dụng không còn chỉ chạy trên các máy chủ vật lý trong các trung tâm dữ liệu của công ty. Hoàn toàn ngược lại, các ứng dụng có thể chạy ở mọi nơi—trên máy chủ vật lý truyền thống, trên máy chủ ảo di động hoặc trên đám mây.
- Không còn khái niệm chu vi mạng truyền thông: Với sự phổ biến của các thiết bị mới, tính di động của ứng dụng và các dịch vụ doanh nghiệp và người tiêu dùng dựa trên đám mây, khái niệm về chu vi mạng tĩnh hầu như đã biến mất.
- Yêu cầu kinh doanh bên ngoài: Doanh nghiệp cũng phải cung cấp cho khách, nhà thầu bên thứ ba và đối tác kinh doanh quyền truy cập mạng bằng nhiều loại thiết bị từ nhiều địa điểm.

Yếu tố trung tâm trong tất cả những thay đổi này là điện toán di động. Các thiết bị di động đã trở thành một yếu tố thiết yếu cho các tổ chức như là một phần của cơ sở hạ tầng mạng tổng thể

2. Bảo mật thiết bị di động

Các nguy cơ an ninh

THIẾU KIỂM SOÁT AN NINH VẬT LÝ: Các thiết bị di động thường nằm dưới sự kiểm soát hoàn toàn của người dùng, đồng thời được sử dụng và lưu giữ ở nhiều vị trí ngoài tầm kiểm soát của tổ chức, bao gồm cả bên ngoài cơ sở.

SỬ DỤNG THIẾT BỊ DI ĐỘNG KHÔNG ĐÁNG TIN Cậy: Ngoài các thiết bị di động do công ty cấp và do công ty kiểm soát, hầu như tất cả nhân viên sẽ có điện thoại thông minh và/hoặc máy tính bảng cá nhân.

SỬ DỤNG MẠNG KHÔNG ĐÁNG TIN Cậy: Nếu thiết bị di động được sử dụng tại cơ sở, thiết bị này có thể kết nối với các tài nguyên của tổ chức qua mạng không dây nội bộ của chính tổ chức. Tuy nhiên, đối với việc sử dụng bên ngoài cơ sở, người dùng thường sẽ truy cập tài nguyên của tổ chức qua Wi-Fi hoặc truy cập di động vào Internet và từ Internet đến tổ chức. Do đó, lưu lượng truy cập bao gồm phân đoạn bên ngoài cơ sở có khả năng dễ bị nghe lén hoặc tấn công theo kiểu trung gian.

SỬ DỤNG ỨNG DỤNG DO CÁC BÊN KHÔNG BIẾT: Theo thiết kế, thật dễ dàng để tìm và cài đặt các ứng dụng của bên thứ ba trên thiết bị di động

2. Bảo mật thiết bị di động

Các nguy cơ an ninh:

TƯƠNG TÁC VỚI CÁC HỆ THỐNG KHÁC: Một tính năng phổ biến được tìm thấy trên điện thoại thông minh và máy tính bảng là khả năng tự động đồng bộ hóa dữ liệu, ứng dụng, danh bạ, ảnh, v.v. với các thiết bị điện toán khác và với bộ lưu trữ dựa trên đám mây.

SỬ DỤNG NỘI DUNG KHÔNG TRUNG THỰC: Thiết bị di động có thể truy cập và sử dụng nội dung mà các thiết bị máy tính khác không gặp phải. Một ví dụ là mã Phản hồi nhanh (QR) độc hại

SỬ DỤNG DỊCH VỤ ĐỊNH VỊ: Khả năng GPS trên thiết bị di động có thể được sử dụng để duy trì kiến thức về vị trí thực tế của thiết bị. Kẻ tấn công có thể sử dụng thông tin vị trí để xác định vị trí của thiết bị và người dùng, thông tin này có thể được sử dụng cho kẻ tấn công.

2. Bảo mật thiết bị di động

Các chiến lược bảo mật thiết bị di động:

BẢO MẬT THIẾT BỊ: Một số tổ chức sẽ cung cấp thiết bị di động cho nhân viên sử dụng và thiết lập cấu hình trước các thiết bị đó để tuân thủ chính sách bảo mật doanh nghiệp. Tuy nhiên, nhiều tổ chức sẽ thấy thuận tiện hoặc thậm chí cần thiết khi áp dụng chính sách mang theo thiết bị của riêng bạn (BYOD: bring your own device) cho phép các thiết bị di động cá nhân của nhân viên có quyền truy cập vào tài nguyên của công ty.

BẢO MẬT LUƯ LƯỢNG: Bảo mật lưu lượng dựa trên các cơ chế mã hóa và xác thực thông thường.

HÀNG RÀO BẢO MẬT: Tổ chức nên có các cơ chế bảo mật để bảo vệ mạng khỏi bị truy cập trái phép. Chiến lược bảo mật cũng có thể bao gồm các chính sách tường lửa dành riêng cho lưu lượng truy cập thiết bị di động.

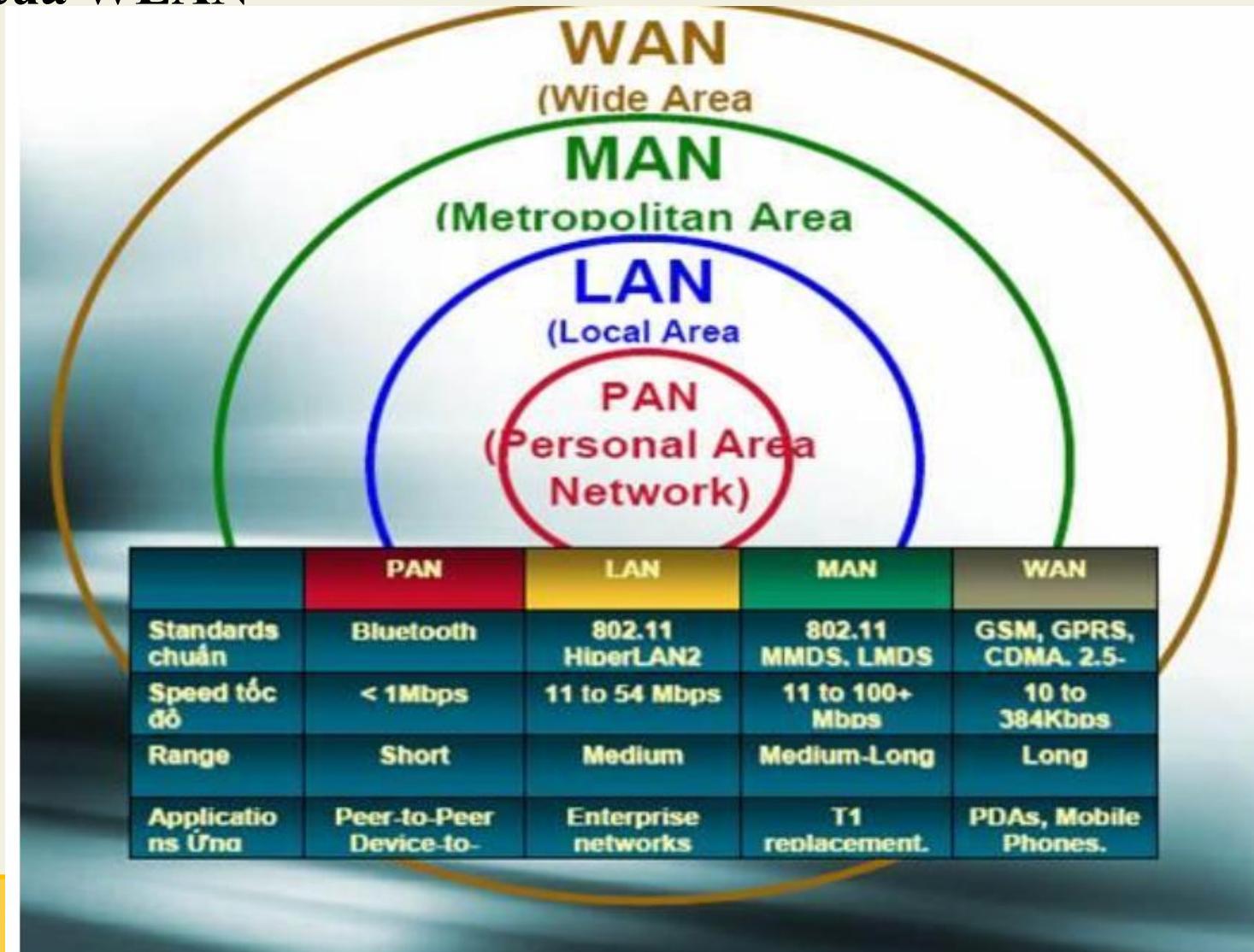
3. Tổng quan về mạng LAN không dây theo IEEE 802.11

- ✓ Năm 1985, Ủy ban liên lạc liên bang Mỹ FCC (*Federal Communications Commission*), quyết định “mở cửa” một số băng tần của giải sóng vô tuyến, cho phép sử dụng chúng mà không cần giấy phép của chính phủ.
- ✓ FCC đã đồng ý “thả” 3 giải sóng công nghiệp, khoa học và y tế cho giới kinh doanh viễn thông.
- ✓ Ba giải sóng này, gọi là các “băng tần rác” (*garbage bands* – 900 MHz, 2,4 GHz, 5,8 GHz), được phân bổ cho các thiết bị sử dụng vào các mục đích ngoài liên lạc

An ninh mạng không dây

3. Tổng quan về mạng LAN không dây (Wireless LAN) theo IEEE 802.11

Vai trò và vị trí của WLAN



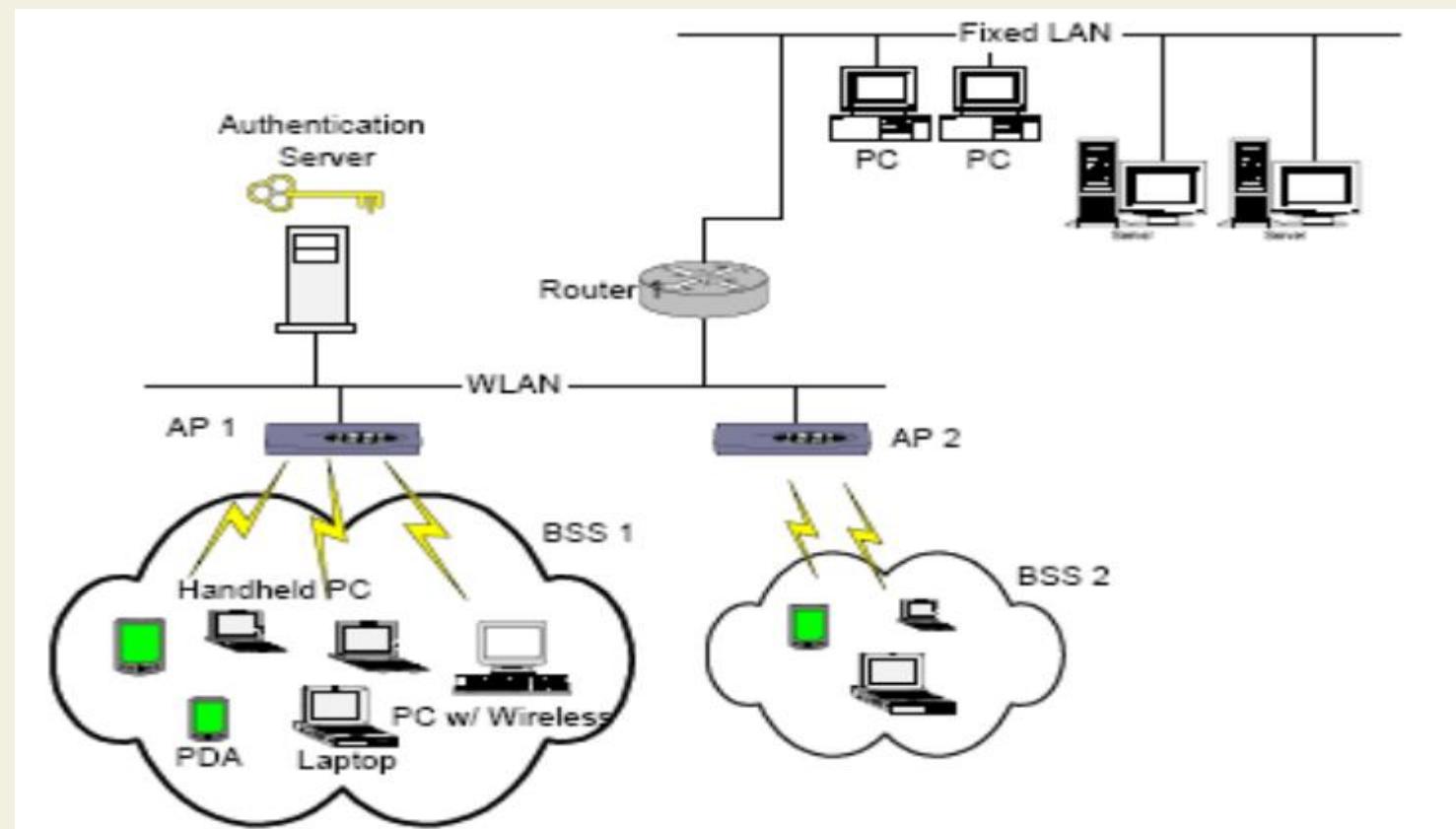
3. Tổng quan về mạng LAN không dây theo IEEE 802.11

- Chuẩn IEEE 802.11 chính thức được ban hành năm 1997.
- IEEE 802.11 (chuẩn WiFi) biểu thị một tập hợp các chuẩn WLAN được phát triển bởi ủy ban chuẩn hóa IEEE LAN/MAN (IEEE 802.11).
- Thuật ngữ 802.11x có thể được sử dụng để biểu thị một tập hợp các chuẩn đối với tất cả các chuẩn thành phần của nó.
- IEEE 802.11 có thể được sử dụng để biểu thị chuẩn 802.11, đôi khi được gọi là 802.11 gốc (*802.11 legacy*).

An ninh mạng không dây

3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Cấu trúc WLAN: Một WLAN thông thường gồm có 2 phần: các thiết bị truy nhập không dây (*Wireless Clients*), các điểm truy nhập (*Access Points – AP*)



3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Các chuẩn bảo mật mạng WLAN:

- **WEP** (Wired Equivalent Privacy) là chuẩn bảo mật wifi lâu đời nhất, ra đời vào năm 1997. Đây được xem là phương thức bảo mật wifi **kém an toàn nhất**. Vào năm 2004, chuẩn bảo mật WEP đã bị **loại bỏ**.
- **WPA** (Wi-Fi Protected Access) là chuẩn bảo mật được phát triển để thay thế WEP do mã hóa WEP đã lỗi thời và dễ dàng bị phá vỡ.
 - WPA có nhiều cải tiến so với WEP như hỗ trợ **TKIP** (Temporal Key Integrity Protocol) để **ngăn chặn** việc **đánh cắp các gói tin truyền trong wifi** và **MIC** (Message Integrity Check) nhằm **đảm bảo dữ liệu không bị giả mạo**. Tuy vậy, WAP vẫn còn tồn đọng một vài lỗ hổng từ WEP.
- **WPA2** là chuẩn bảo mật thay thế cho WPA kể từ năm 2006. WPA2 còn thay thế TKIP bằng **giao thức CCMP** (Counter Mode Cipher Block Chaining Message Authentication Code Protocol).
 - CCMP là một giao thức truyền dữ liệu và kiểm soát tính truyền dữ liệu thông nhất để **bảo đảm cả tính bảo mật và nguyên vẹn** của dữ liệu được truyền đi. Hiện nay, phần lớn bộ định tuyến wifi đều sử dụng WPA2.
- **WPA3** là chuẩn bảo mật wifi **mới nhất** hiện nay và được áp dụng trên một số bộ định tuyến sản xuất trong năm 2019. WPA3 được nâng cấp tối ưu hơn so với chuẩn bảo mật WPA2.

3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Các dịch vụ 802.11i

- **Xác thực:** Một giao thức được sử dụng để xác định trao đổi giữa người dùng và AS cung cấp xác thực lẫn nhau và tạo các khóa tạm thời được sử dụng giữa máy khách và AP qua liên kết không dây.
- **Kiểm soát truy cập:** Chức năng này thực thi việc sử dụng chức năng xác thực, định tuyến các bản tin đúng cách và tạo điều kiện trao đổi khóa. Nó có thể hoạt động với nhiều giao thức xác thực.
- **Quyền riêng tư với tính toàn vẹn của thông báo:** Dữ liệu được mã hóa cùng với mã toàn vẹn của thông báo để đảm bảo rằng dữ liệu không bị thay đổi.

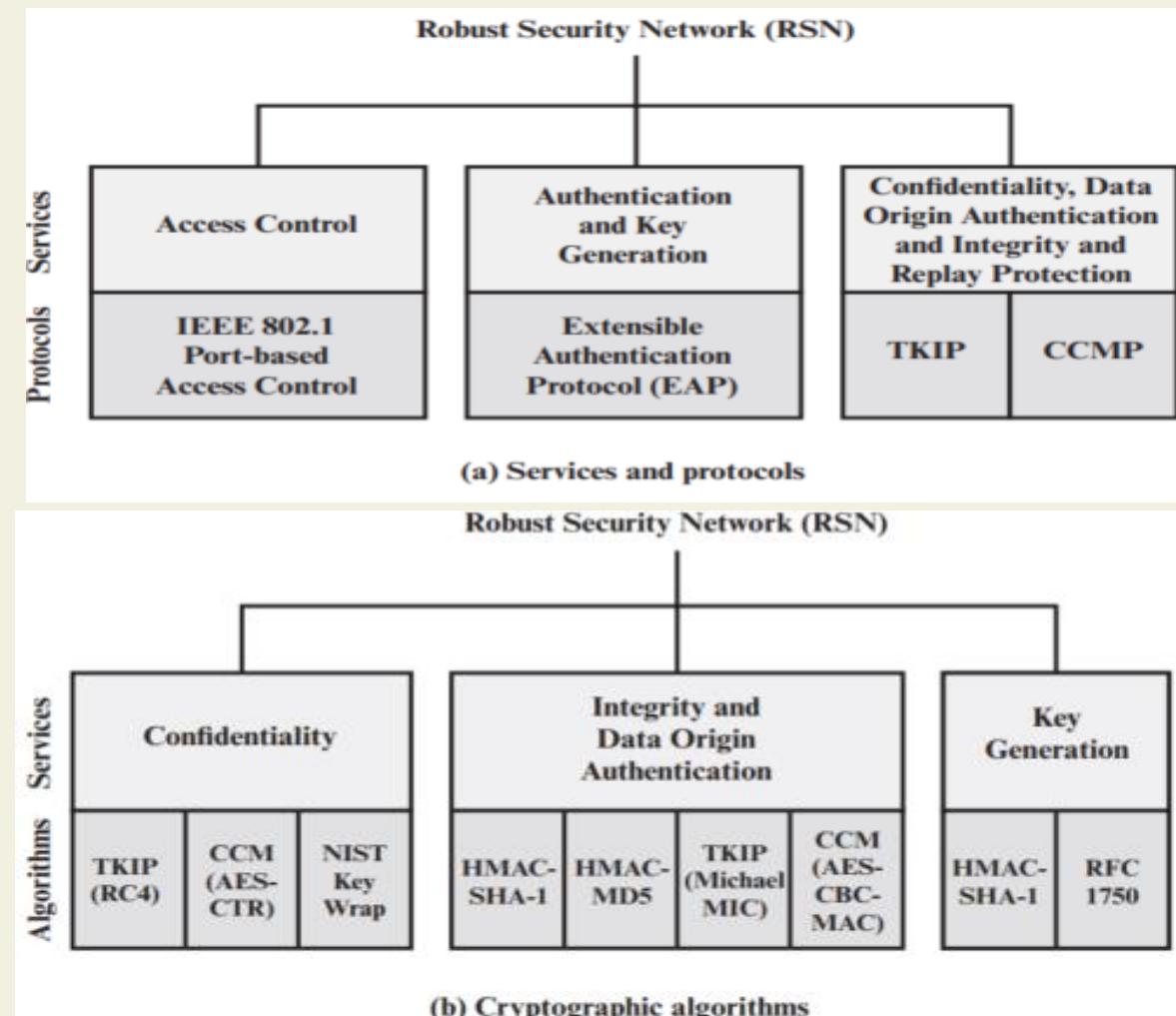


Figure 7.6 Elements of IEEE 802.11i

3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Các pha hoạt động của IEEE 802.11i: 5 pha

- 1- Khám phá -Discovery
- 2- Xác thực - Authentication
- 3 – Tạo và phân phối khóa - Key generation and distribution
- 4 – Truyền dữ liệu được bảo vệ - Protected data transfer
- 5 – Kết thúc kết nối - Connection termination

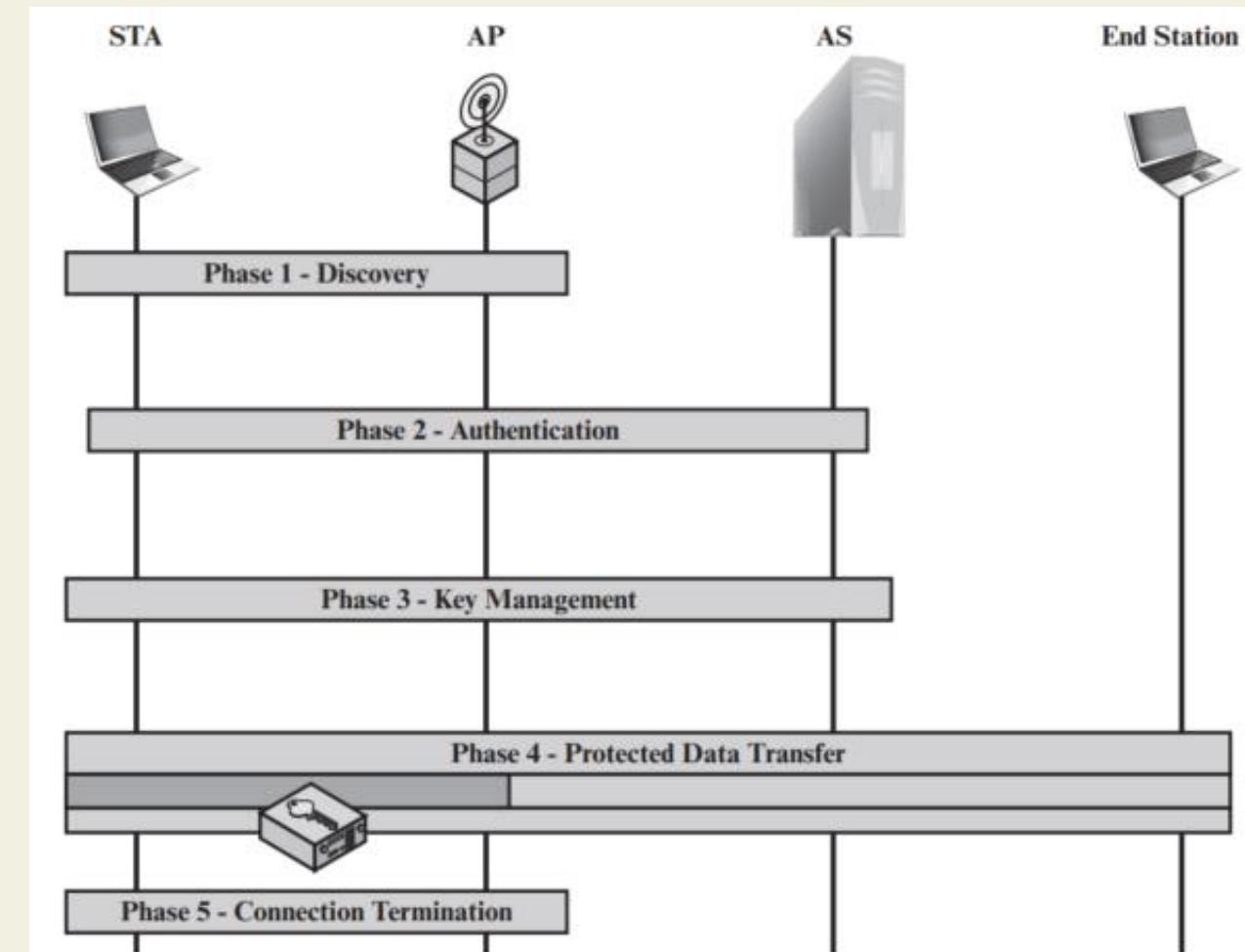
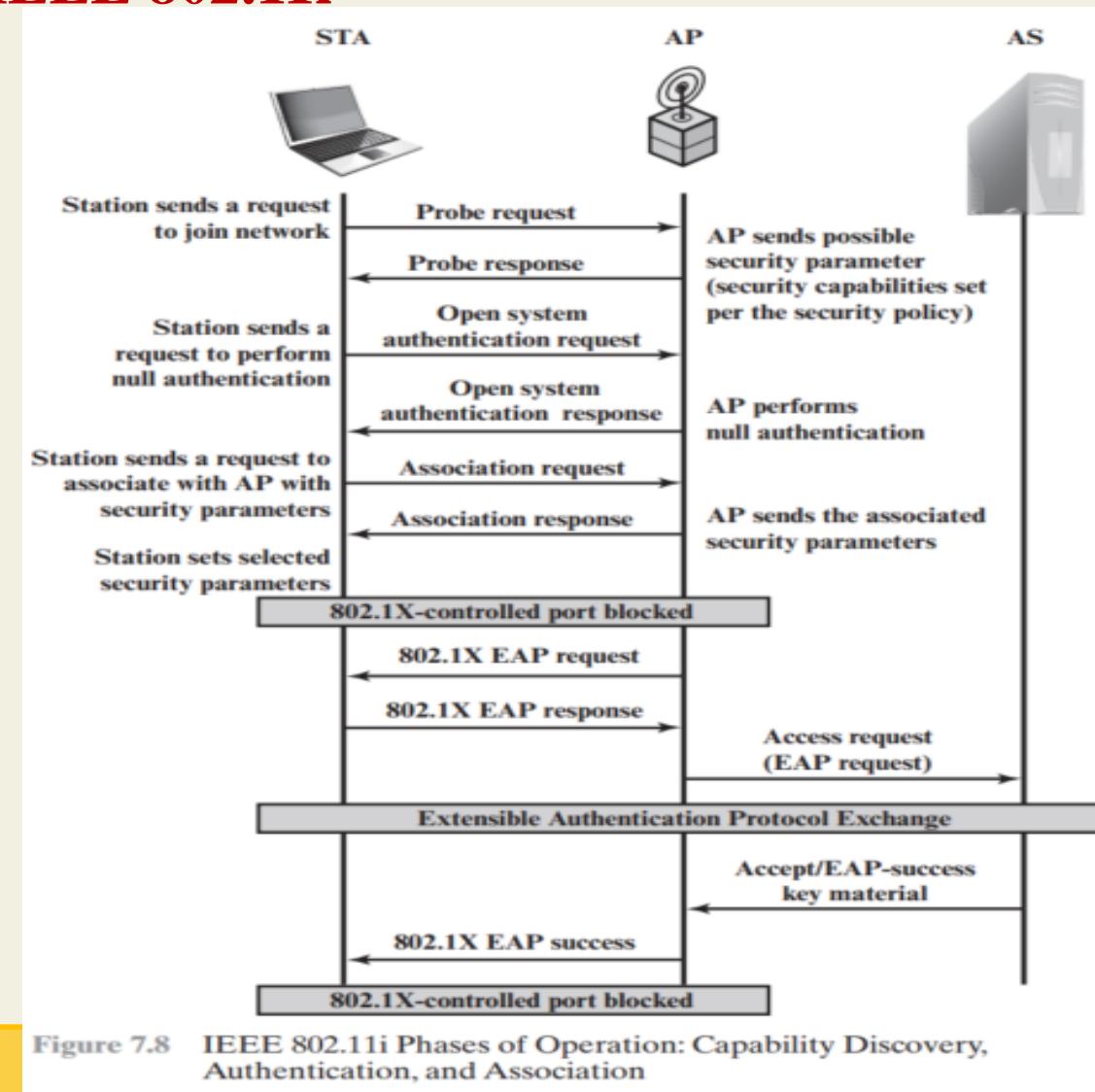


Figure 7.7 IEEE 802.11i Phases of Operation

An ninh mạng không dây

3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Các pha hoạt động của IEEE 802.11i

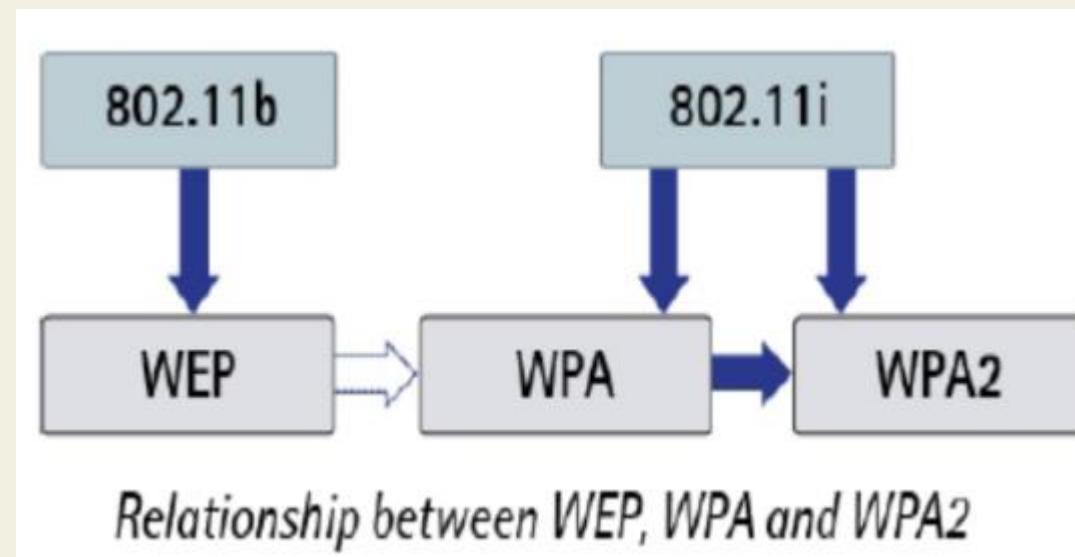


An ninh mạng không dây

3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Wi-Fi Protected Access –WPA/WPA2

Vào tháng 10/2002, WPA ra đời như một giải pháp bảo mật tăng cường cho WLAN



An ninh mạng không dây

3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Wi-Fi Protected Access –WPA/WPA2

WPA đã làm tăng rất nhiều mức độ bảo vệ dữ liệu và điều khiển truy nhập cho các mạng WLAN đang tồn tại, nó đã giải quyết tất cả các vấn đề về các nguy cơ tổn thương trong giải pháp WLAN trước đó. Và nó được dùng để thay thế hoàn toàn WEP trong đảm bảo an toàn WLAN.

WPA cung cấp bảo mật cho tất cả các phiên bản đã tồn tại của các thiết bị WLAN 802.11: a, b, nó cũng được thiết kế để tối thiểu hóa sự ảnh hưởng đến hiệu năng hoạt động của mạng.

WPA cung cấp việc bảo mật dữ liệu ở mức độ cao và chỉ những người dùng có quyền mới có thể truy nhập mạng nhờ một thuật toán mã hóa mạnh và khả năng xác thực mạnh

An ninh mạng không dây

3. Tổng quan về mạng LAN không dây theo IEEE 802.11

Hoạt động của WPA

- ▶ Sử dụng TKIP để mã hóa (Temporary Key Integrity Protocol), sử dụng xác thực 802.1x với giao thức xác thực mở rộng EAP.
- ▶ TKIP sử dụng thuật toán RC4 đối với thiết kế chuẩn, một số nhà cung cấp có thể cung cấp AES như là một lựa chọn trong các sản phẩm WPA của họ.
- ▶ WPA sử dụng 48 bit IV thay cho 24 bit IV, nó làm tăng đáng kể mức an toàn.
- ▶ WPA có thể sử dụng khóa mới cho mỗi 802.11 frame, hoặc có thể dựa trên một thời khoảng được xác định trước trên AP.
- ▶ Sử dụng 8 byte MIC (Michael Message Integrity Check) để kiểm tra tính toàn vẹn bản tin.
- ▶ WPA sử dụng chuỗi IV để bảo vệ tấn công lặp lại.
- ▶ Giải pháp xác thực dựa trên 802.1X được tích hợp trong mỗi sản phẩm.
- ▶ WPA hỗ trợ sử dụng phương án EAP hoặc PSK để xác thực người dùng trong mạng.

- **TKIP**

WPA được xây dựng tương thích hoàn toàn với các thiết bị WLAN đang tồn tại. TKIP tăng nâng cao khả

năng bảo mật và phải tuân theo các yêu cầu tương thích, vì vậy nó cũng sử dụng thuật toán mật mã dòng RC4. Vì vậy để sử dụng TKIP chỉ cần nâng cấp phần mềm. Trong thực tế hầu hết các chuyên gia tin rằng TKIP là một giải pháp mã hóa mạnh hơn WEP. Tuy nhiên họ

cũng đồng ý rằng TKIP chỉ là một giải pháp tạm thời vì nó sử dụng RC4. Ưu điểm chính của TKIP so với WEP là sự luân phiên khóa.

- Trên thực tế, TKIP bao gồm 4 thuật toán để thực hiện tốt nhất các khả năng an toàn

Câu hỏi ôn tập?

Tài liệu tham khảo chính

Mô hình mạng an toàn và phần mềm độc hại

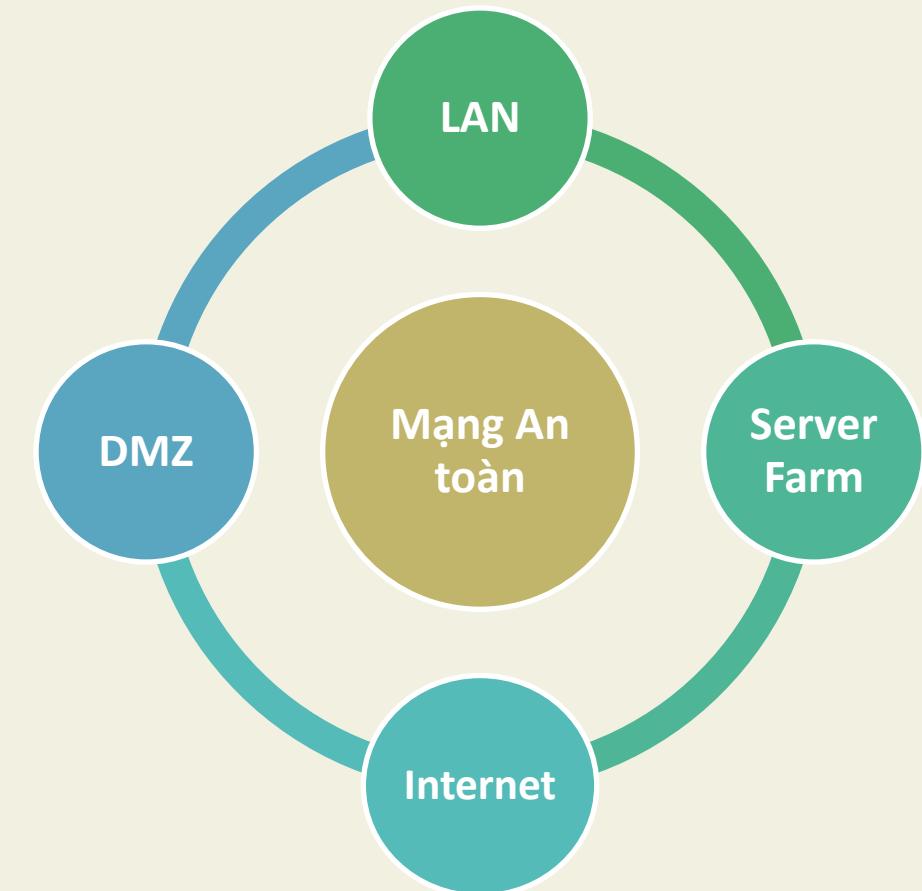
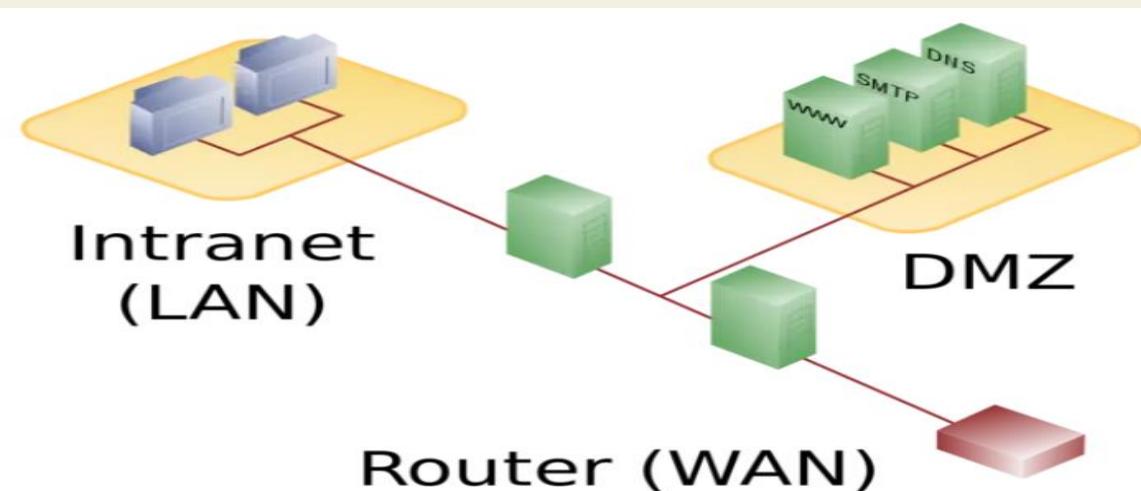
Nội dung chính:

- Giới thiệu chung về mô hình mạng an toàn
- Demilitarized Zone (DMZ)
- Network Address Translation (NAT)
- Mạng LAN ảo (VLAN)
- Mã độc

Mô hình mạng an toàn

Mô hình mạng an toàn là cần thiết cho mỗi tổ chức để phân biệt rõ ràng giữa các vùng mạng theo chức năng và thiết lập các chính sách an toàn thông tin riêng cho từng vùng mạng theo yêu cầu thực tế.

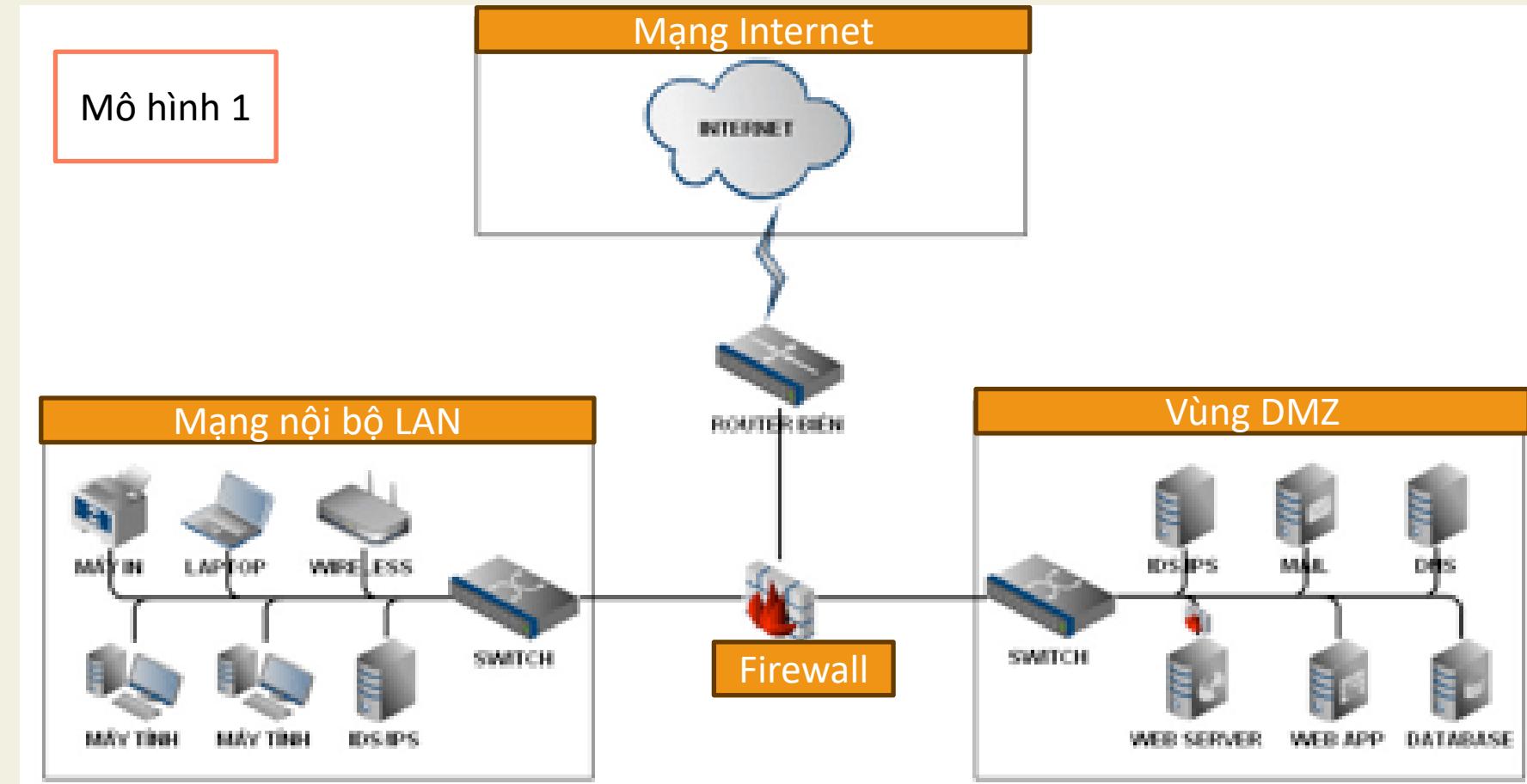
- ✓ Việc tổ chức mô hình mạng an toàn đảm bảo bảo mật có ảnh hưởng lớn đến sự an toàn cho các hệ thống mạng và các cổng thông tin điện tử.
- ✓ Là cơ sở đầu tiên cho việc xây dựng các hệ thống phòng thủ và bảo vệ.
- ✓ Tổ chức mô hình mạng an toàn có thể hạn chế được các tấn công từ bên trong và bên ngoài một cách hiệu quả.



Một số mô hình mạng phổ biến

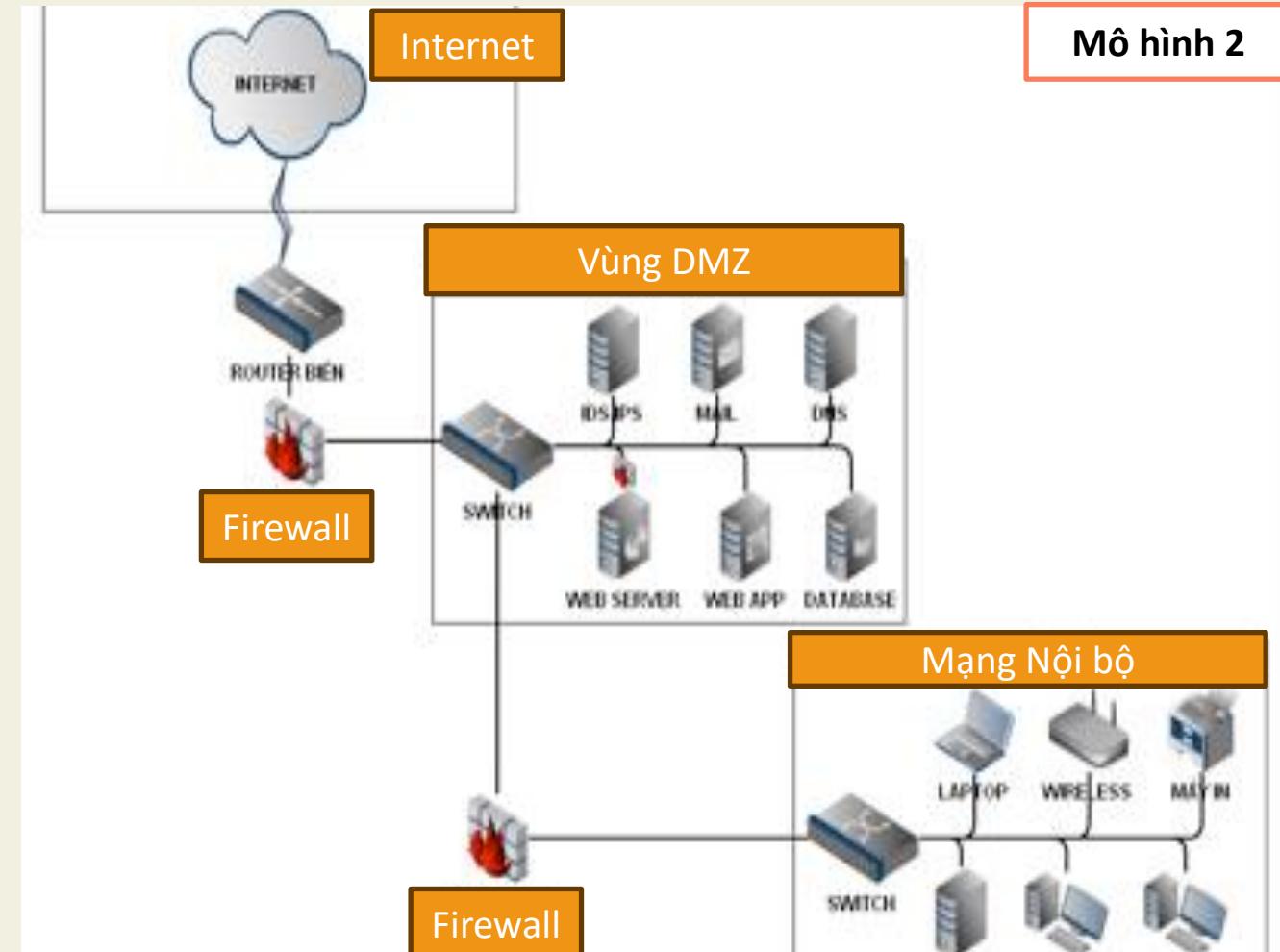
- ✓ Vùng mạng Internet, vùng mạng nội bộ và vùng mạng DMZ được thiết kế tách biệt nhau.
- ✓ Firewall được đặt ở giữa các vùng mạng nhằm kiểm soát luồng thông tin giữa các vùng mạng với nhau và bảo vệ các vùng mạng khỏi các tấn công trái phép.

Mô hình 1



Một số mô hình mạng phổ biến

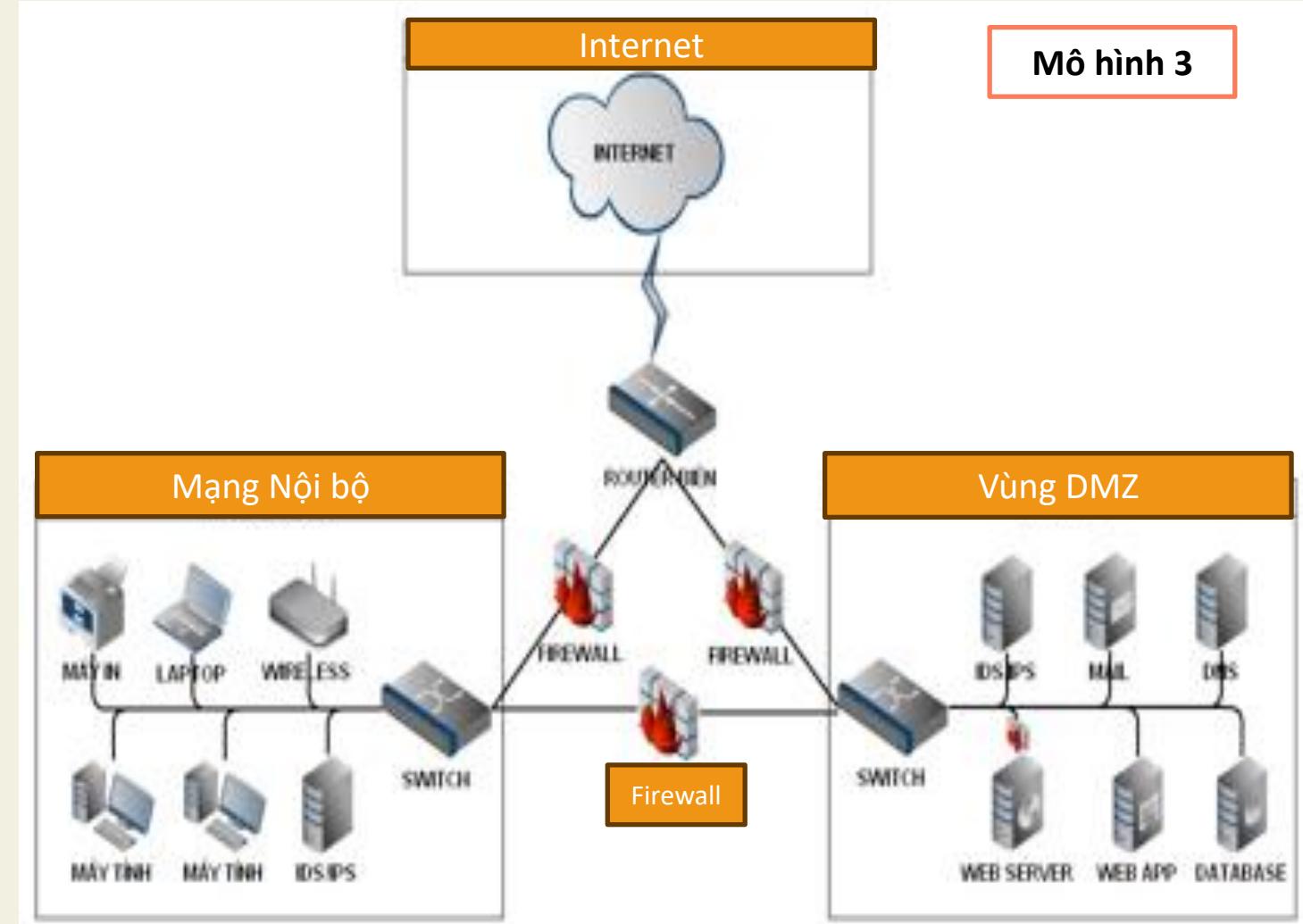
- ✓ Một firewall giữa vùng mạng Internet và vùng mạng DMZ và một firewall giữa vùng mạng DMZ và vùng mạng nội bộ.
- ✓ Vùng mạng nội bộ nằm sâu bên trong và cách vùng mạng Internet bằng 2 lớp firewall



Mô hình mạng an toàn

Một số mô hình mạng phổ biến

- ✓ Một firewall giữa vùng mạng Internet và vùng mạng DMZ
- ✓ Một firewall giữa vùng mạng DMZ và vùng mạng nội bộ
- ✓ Một firewall giữa vùng mạng nội bộ và vùng mạng Internet



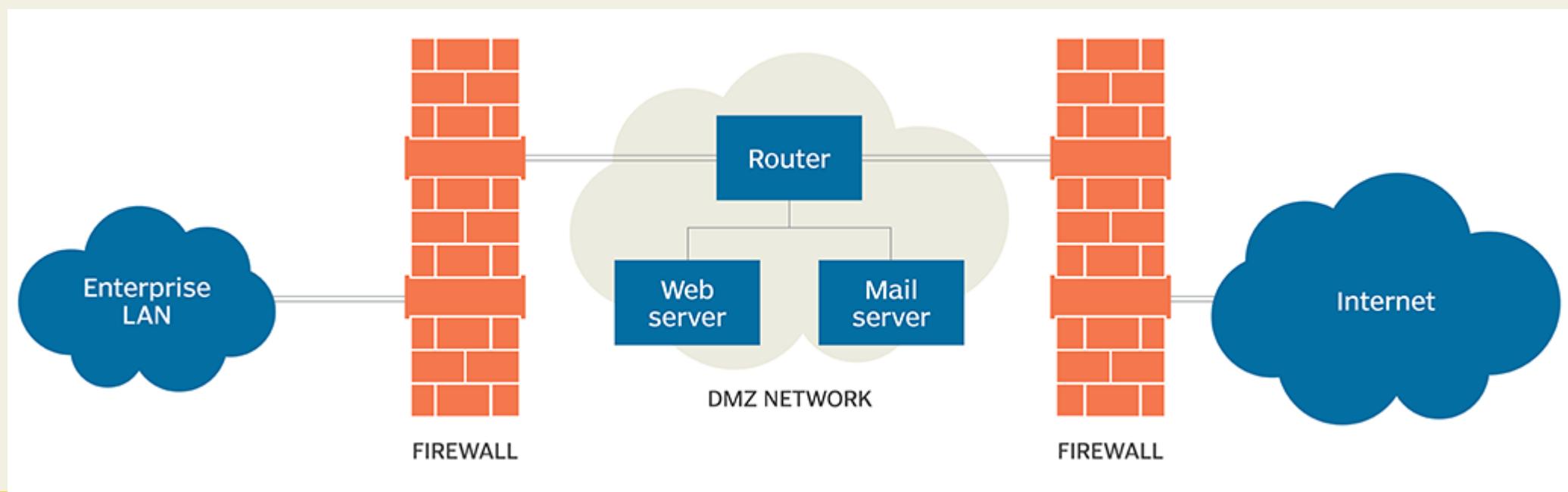
Một số tiêu chí khi thiết kế mô hình mạng an toàn

- ✓ Nên đặt các máy chủ web, máy chủ thư điện tử (mail server)... cung cấp dịch vụ ra mạng Internet trong vùng mạng DMZ;
- ✓ Các máy chủ không trực tiếp cung cấp dịch vụ ra mạng ngoài như máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ xác thực...;
- ✓ Nên thiết lập các hệ thống phòng thủ như tường lửa (firewall) và thiết bị phát hiện/phòng chống xâm nhập (**IDS/IPS**) để bảo vệ hệ thống, chống tấn công và xâm nhập trái phép;
- ✓ Nên đặt một Router ngoài cùng (Router biên) trước khi kết nối đến nhà cung cấp dịch vụ internet (ISP) để lọc một số lưu lượng không mong muốn và chặn những gói tin đến từ những địa chỉ IP không hợp lệ.

DMZ - Demilitarized Zone

Định nghĩa: Trong mạng máy tính, DMZ hay khu vực phi quân sự là một mạng con vật lý hoặc logic ngăn cách mạng cục bộ (LAN) với các mạng không đáng tin cậy khác -- thường là internet công cộng.

DMZ là nơi chứa các server và cung cấp các service cho các host trong LAN cũng như các host từ các LAN bên ngoài. Là bước cuối cùng các packet qua trước khi truyền vào internet, và cũng là nơi đầu tiên packet đến trước khi vào mạng LAN



DMZ - Demilitarized Zone

- ✓ Hệ thống mạng nội thường bao gồm các server cung cấp các dịch vụ cơ bản như: *Directory service*(*Active Directory, OpenLDAP...*), *DNS, DHCP, File/Print Sharing, Web, Mail, FTP*.
- ✓ Trong đó thì các server Web, Mail, FTP thường phải cung cấp các dịch vụ của chúng cho cả những người dùng nằm bên trong lẫn bên ngoài mạng nội bộ.
- ✓ Nếu hacker từ mạng bên ngoài kiểm soát được các public server như Web, Mail, FTP?
- ✓ Rất có thể hacker sẽ dựa vào các server đã bị chiếm đoạt này để đánh vào các server khác (như DNS, DHCP, Directory Service...) cũng như thâm nhập sâu hơn vào các máy trạm bên trong.
→ DMZ sẽ giảm thiệt hại cho các host của LAN

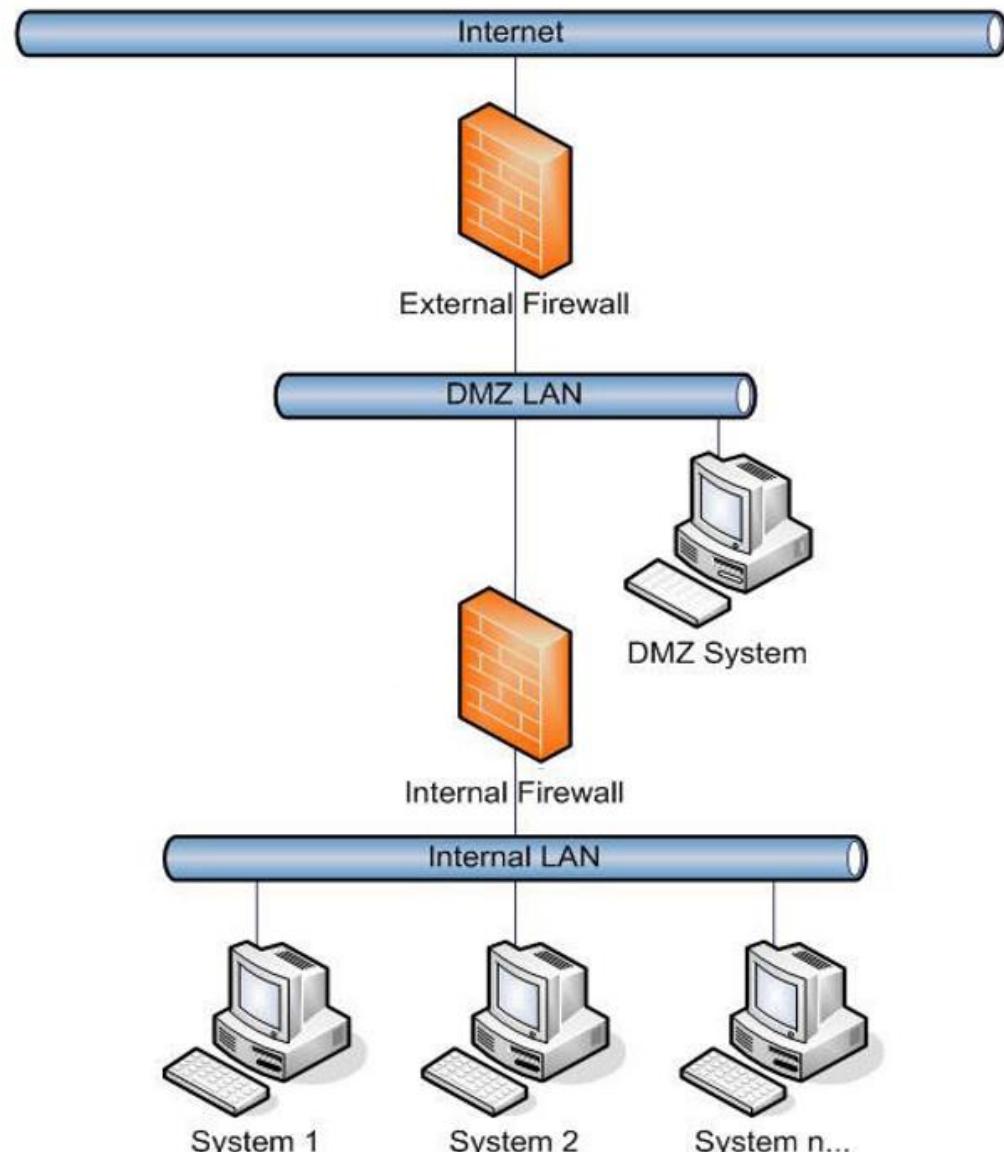
Vai trò của DMZ trong vùng mạng:

- DMZ là nơi chứa các thông tin cho phép người dùng từ internet truy xuất vào và chấp nhận các rủi ro tấn công từ internet.
- Các dịch vụ thường được triển khai trong vùng DMZ là: Mail, Web, FTP

DMZ - Demilitarized Zone

Thiết lập vùng mạng DMZ: 02 cách

C1: Đặt DMZ giữa 2 firewall, một để lọc các thông tin từ internet vào và một để kiểm tra các luồng thông tin vào mạng cục bộ.

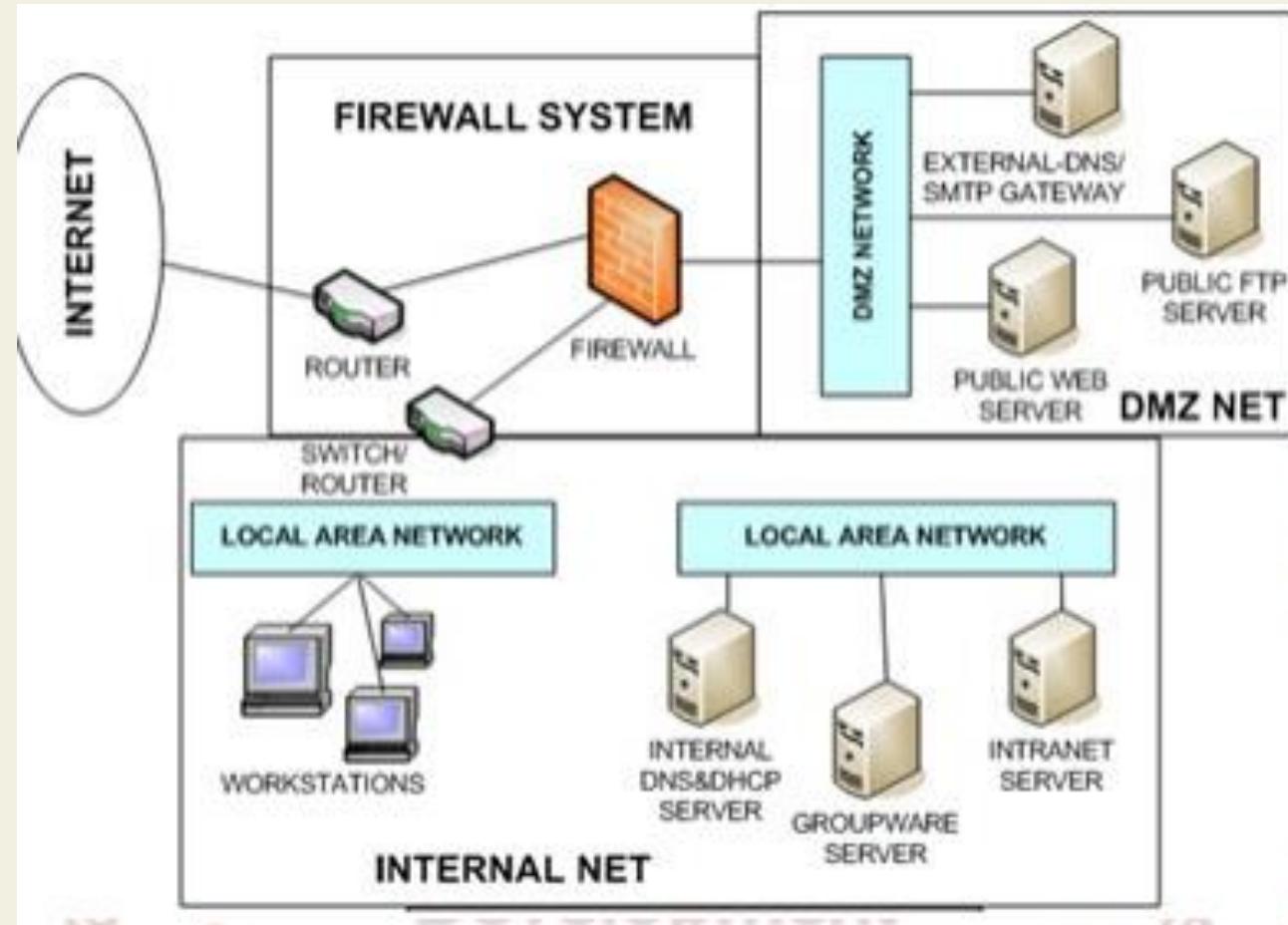


DMZ - Demilitarized Zone

Thiết lập vùng mạng DMZ: 02 cách

C2: Sử dụng Router có nhiều cổng để đặt vùng DMZ vào một nhánh riêng tách rời với mạng cục bộ.

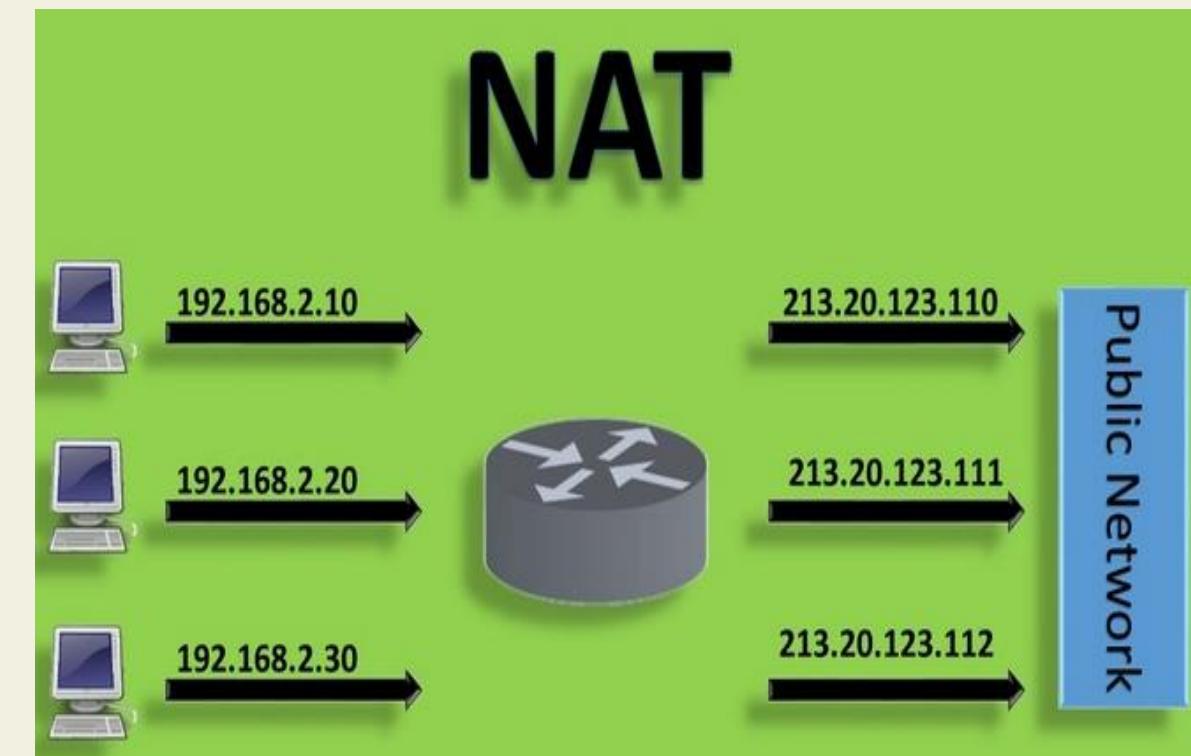
Cách thiết lập nào an toàn hơn? Vì sao?



NAT - Network Address Translation

Định nghĩa:

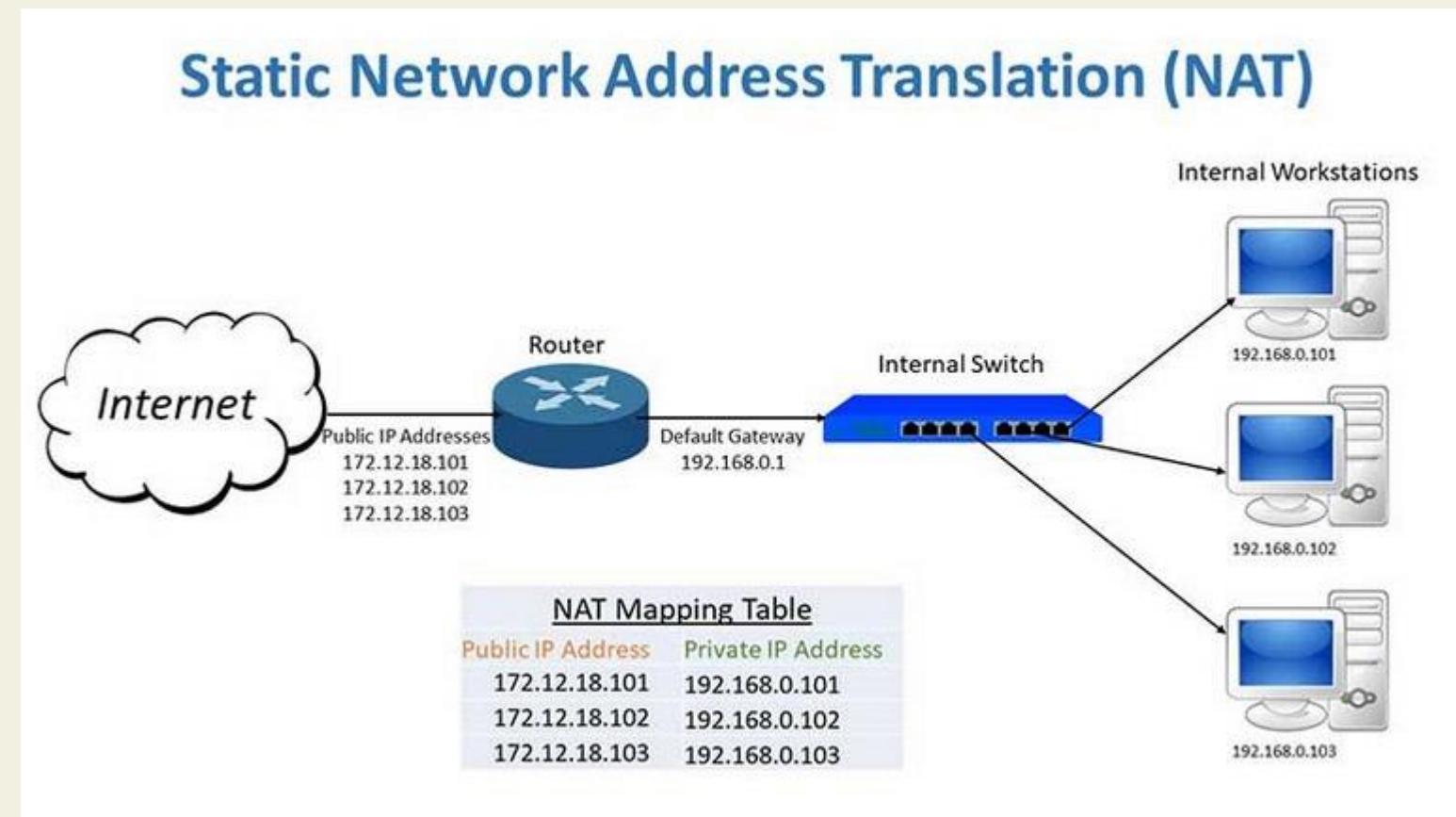
- NAT là một kỹ thuật chuyển đổi đặc biệt, NAT cho phép một hoặc nhiều địa chỉ IP mạng cục bộ (Private) (IP nội miền) chuyển đổi sang một hoặc nhiều địa chỉ IP mạng công cộng (Internet) (IP ngoại miền).
- Vị trí thực hiện kỹ thuật NAT là tại Router biên, nơi kết nối hai loại mạng này.



NAT - Network Address Translation

Chức năng chính của NAT trong hệ thống mạng

- Trong một hệ thống mạng NAT giữ vai trò di chuyển gói tin giữa các lớp mạng khác nhau.
- Cụ thể, NAT cần tiến hành chuyển đổi địa chỉ IP trong từng gói tin và chuyển đến router cùng một số thiết bị mạng khác.



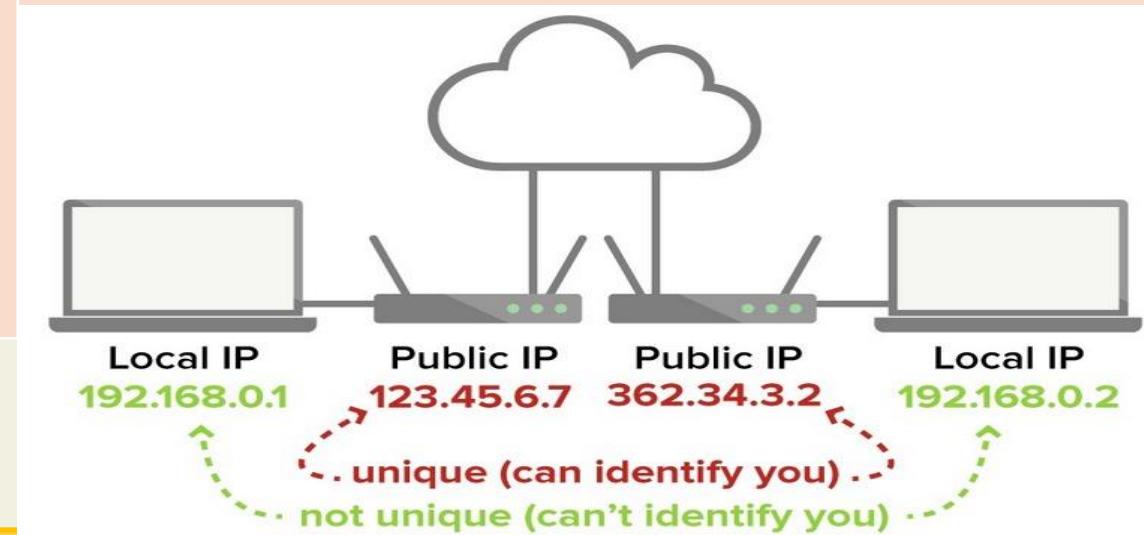
NAT - Network Address Translation

Ưu điểm và nhược điểm của NAT

Ưu điểm	Nhược điểm
<ul style="list-style-type: none">✓ Tiết kiệm địa chỉ IPv4: Lượng người dùng truy cập internet ngày càng tăng cao. Điều này dẫn đến nguy cơ thiếu hụt địa chỉ IPv4. Kỹ thuật NAT sẽ giúp giảm thiểu được số lượng địa chỉ IP cần sử dụng.✓ Giúp che giấu IP bên trong mạng LAN.✓ NAT có thể chia sẻ kết nối internet cho nhiều máy tính, thiết bị di động khác nhau trong mạng LAN chỉ với một địa chỉ IP public duy nhất.✓ NAT giúp nhà quản trị mạng lọc được các gói tin đến và xét duyệt quyền truy cập của IP public đến 1 port bất kỳ.	<ul style="list-style-type: none">✓ Khi dùng kỹ thuật NAT, CPU sẽ phải kiểm tra và tốn thời gian để thay đổi địa chỉ IP. Điều này làm tăng độ trễ trong quá trình switching. Làm ảnh hưởng đến tốc độ đường truyền của mạng internet.✓ NAT có khả năng che giấu địa chỉ IP trong mạng LAN nên kỹ thuật viên sẽ gặp khó khăn khi cần kiểm tra nguồn gốc IP hoặc truy tìm dấu vết của gói tin.✓ NAT giấu địa chỉ IP nên sẽ khiến cho 1 vài ứng dụng cần sử dụng IP không thể hoạt động được.

NAT - Địa chỉ IP Private và IP Public

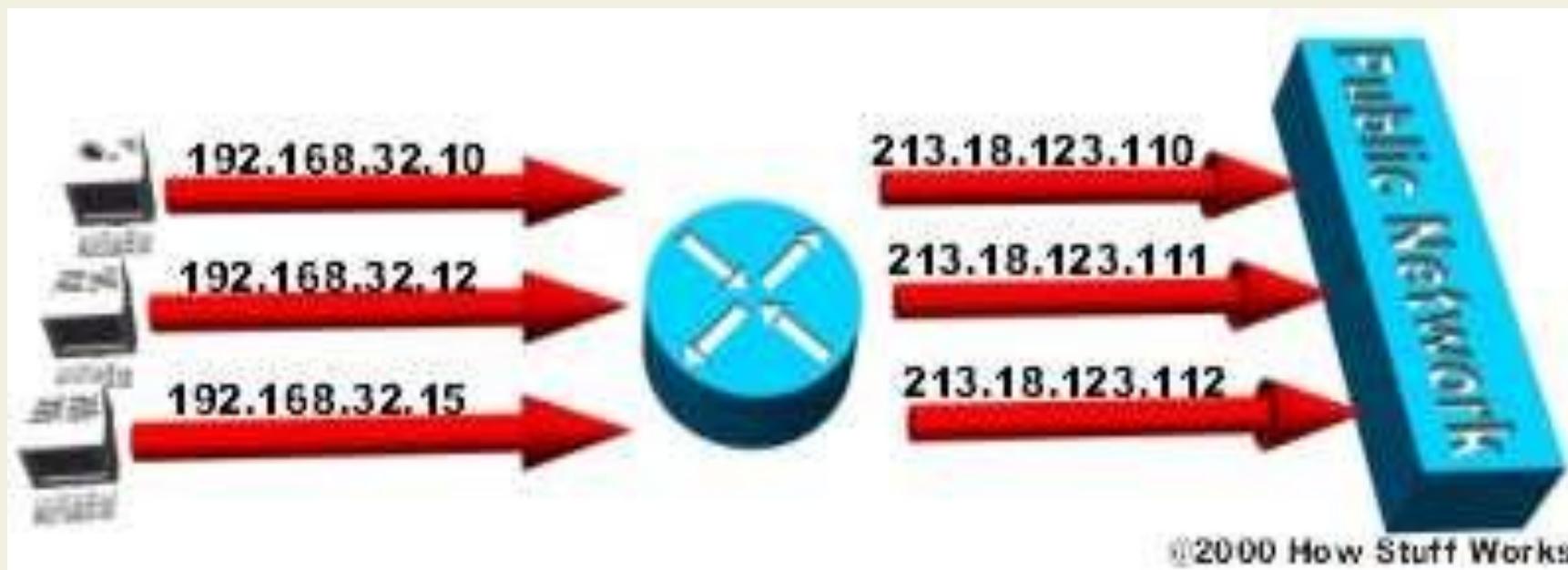
IP Private	IP Public
<ul style="list-style-type: none">✓ Mỗi một máy thiết bị trong mạng nội bộ (mạng LAN) của các công ty, tổ chức, trường học,... sẽ có 1 IP Private riêng.✓ Các IP Private trong cùng hệ thống mạng LAN có thể kết nối với nhau thông qua thiết bị mạng router nhưng không thể kết nối trực tiếp với mạng internet bên ngoài.✓ Muốn kết nối được, các IP Private này phải chuyển đổi thành địa chỉ IP Public thông qua kỹ thuật NAT.✓ IP Private có thể bị trùng lặp khi được kết nối với các IP Public khác nhau✓ IP Private được tùy chỉnh trong LAN theo nguyên tắc thống nhất mà người quản trị mạng đưa ra	<ul style="list-style-type: none">✓ Địa chỉ Public (IP Public) hay còn gọi là IP ngoại miền là một loại địa chỉ được cung cấp bởi các tổ chức có thẩm quyền (ví dụ như nhà cung cấp mạng internet).✓ IP Public là duy nhất✓ IP Public được cung cấp bởi đơn vị cung cấp mạng internet và người dùng không thể tự ý thay đổi.



NAT – Phân loại

03 loại – Static NAT, Dynamic NAT, NAT Overload

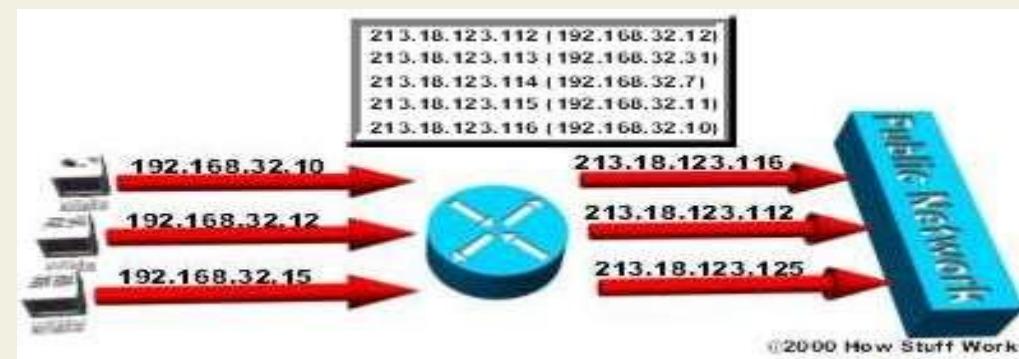
Static NAT - kỹ thuật biến đổi IP này thành IP khác thông qua *cách cố định* từ IP Private sang IP Public. Quy trình này sẽ thực hiện hoàn toàn *thủ công*. Static NAT đặc biệt phát huy tác dụng khi thiết bị sở hữu địa chỉ cố định truy cập internet từ bên ngoài.



NAT – Phân loại

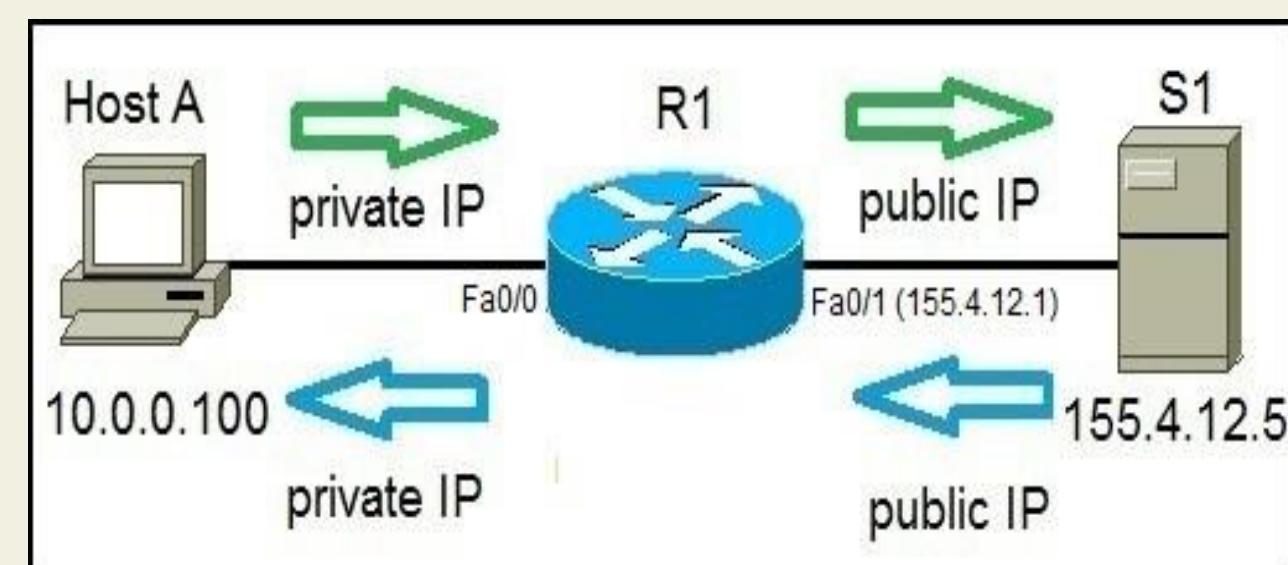
03 loại – Static NAT, Dynamic NAT, NAT Overload

Dynamic NAT: Đây là kỹ thuật chuyển đổi từ một địa chỉ IP sang kiểu IP khác hoàn toàn tự động



- ✓ Host A gửi request để truy cập tài nguyên web từ server internet S1
- ✓ Host A sử dụng địa chỉ IP private khi gửi Request tới R1

- ✓ R1 nhận Request, thay đổi private IP thành địa chỉ global trong pool và gửi Request tới S1
- ✓ S1 trả lời Respond tới R1, R1 sẽ kiểm tra trong bảng NAT của nó và thay đổi địa chỉ IP nhận thành địa chỉ private IP của Host A

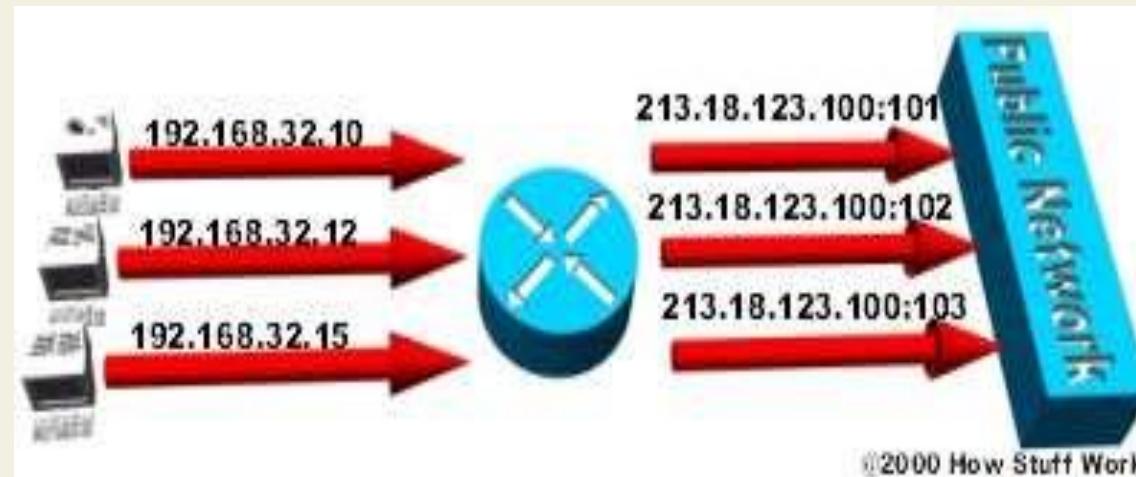


NAT – Phân loại

03 loại – Static NAT, Dynamic NAT, NAT Overload

NAT Overload – còn có tên gọi khác là PAT (Port Address Translation) đây là một kiểu giao thức của NAT động. Nó cũng thực hiện chuyển đổi địa chỉ IP một cách tự động

Overload là dạng many – to – one (ánh xạ nhiều địa chỉ IP thành 1 địa chỉ IP) và dùng các chỉ số cổng (port) khác nhau để phân biệt cho từng chuyển đổi.



Mạng LAN ảo – Virtual LAN

Định nghĩa: là một mạng tùy chỉnh, được tạo từ một hay nhiều mạng cục bộ khác (LAN). Mạng VLAN cho phép một nhóm thiết bị khả dụng trong nhiều mạng được kết hợp với nhau thành một mạng logic. Từ đó tạo ra một mạng LAN ảo (Virtual LAN), được quản lý giống như một mạng LAN vật lý.

- ✓ Virtual LAN ở trong mạng được xác định bằng một con số. Giá trị của con số trên có thể nằm từ 1 đến 4094. Trên một VLAN switch, ta có thể gán các cổng với số VLAN thích hợp.
- ✓ Virtual LAN cung cấp cấu trúc cho phép tạo các nhóm thiết bị, kể cả khi mạng của chúng có khác nhau.
- ✓ **Điểm khác biệt lớn nhất giữa LAN và Virtual LAN:** Trong LAN, các gói mạng được broadcast đến từng thiết bị. Còn trong Virtual LAN thì các gói này chỉ được gửi đến một broadcast domain cụ thể.

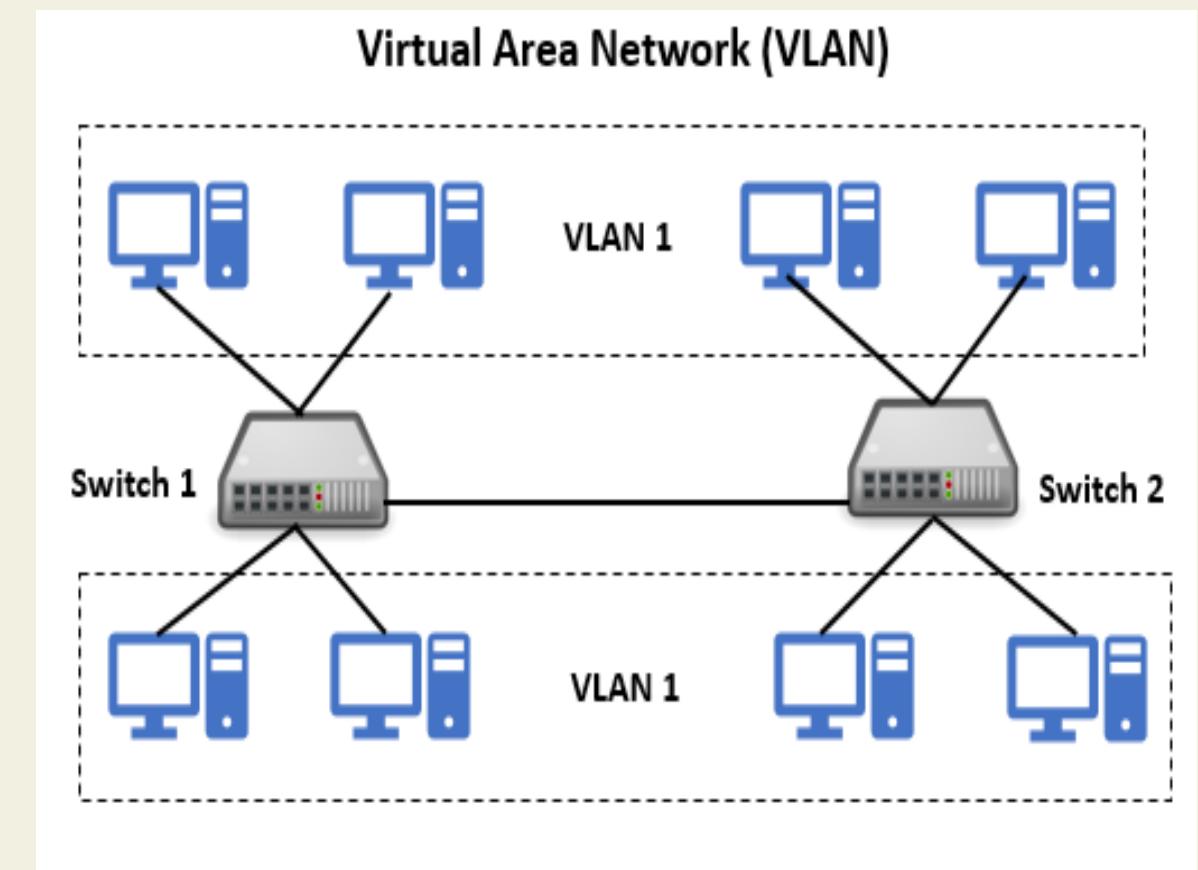
Mạng LAN ảo

Phân loại VLAN

Port - based VLAN: là VLAN dựa trên cổng (port) hoặc VLAN dựa trên giao diện (interface)
→ Sử dụng nhiều

MAC address based VLAN: để cập đến việc gắn các VLAN theo địa chỉ MAC - mỗi địa chỉ MAC được đánh dấu với một VLAN → Ít sử dụng

Protocol - based VLAN: ách cấu hình này tương tự như MAC address based VLAN, nhưng chỉ dùng duy nhất một địa chỉ IP hoặc địa chỉ logic thay thế cho địa chỉ MAC → Ít sử dụng



Mạng LAN ảo

Ứng dụng và lợi ích của VLAN

Tiết kiệm băng thông của hệ thống mạng	Tăng khả năng bảo mật	Có tính linh động cao	Dễ dàng thêm / bớt máy tính vào VLAN
VLAN chia mạng cục bộ (LAN) thành nhiều phân đoạn (segment) mạng nhỏ. Khi có gói tin quảng bá (broadcast), nó sẽ truyền trong VLAN tương ứng. Do đó, việc phân đoạn VLAN giúp tối ưu băng thông của hệ thống mạng.	Các thiết bị ở các VLAN khác nhau sẽ không thể kết nối với nhau (trừ khi trang bị Router nối giữa các VLAN). Ví dụ máy tính ở mạng VLAN kế toán không thể kết nối với các máy tính ở VLAN kỹ sư. Điều này giúp tăng cường bảo mật dữ liệu hiệu quả hơn.	VLAN có thể dễ dàng di chuyển các thiết bị. VLAN có thể được cấu hình tĩnh hoặc động. Trong cấu hình tĩnh, người quản trị mạng sẽ cấu hình cho từng cổng của mỗi Switch. Tiếp đó, gán vào một VLAN bất kỳ. Với cấu hình động, mỗi cổng của Switch có thể tự cấu hình cho VLAN thông qua địa chỉ MAC được thiết bị kết nối vào.	Chỉ cần cấu hình cổng máy tính vào VLAN mong muốn là có thể thêm máy tính vào VLAN.

Mạng LAN ảo

Tiêu chí	VLAN	LAN
Khái niệm	Là một mạng LAN ảo được tạo thành từ một hay nhiều mạng LAN.	Là một tập hợp các máy tính và thiết bị ngoại vi được kết nối trong một phạm vi địa lý nhỏ.
Cách thức hoạt động	Các gói mạng trong VLAN chỉ được gửi đến một địa chỉ Broadcast duy nhất.	Các gói mạng được Broadcast gửi tới từng thiết bị trong mạng LAN.
Giao thức	VLAN sử dụng các giao thức VTP và ISP.	LAN sử dụng giao thức FDDI
Độ trễ	Độ trễ của VLAN giảm xuống thấp hơn LAN	Độ trễ của LAN lớn hơn VLAN
Chi phí	Thấp hơn (do không cần thiết sử dụng Router)	Cao hơn (do cần trang bị Router)
Hiệu suất	VLAN mang lại hiệu suất tốt hơn so với mạng LAN	LAN mang đến hiệu suất thấp hơn so với mạng VLAN
Mức độ an toàn	VLAN an toàn hơn	LAN có mức độ an toàn kém hơn VLAN

Report 2022, Bkav

TOP 5 MÃ ĐỘC PHỔ BIẾN TẤN CÔNG HÀNG TRIỆU MÁY TÍNH TẠI VIỆT NAM



Giới thiệu Malware

- **Malware (Malicious software)** hay còn gọi là mã độc (Malicious code) là tên gọi chung cho các phần mềm được thiết kế, lập trình đặc biệt để gây hại cho máy tính hoặc làm gián đoạn môi trường hoạt động mạng. Mã độc có thể được phát triển với các mục tiêu độc hại như đánh cắp thông tin cá nhân, gây hỏng hóc hệ thống, hoặc theo dõi hoạt động người dùng mà không được sự cho phép của họ.
- Mã độc thâm nhập vào một hệ thống máy tính mà không có sự đồng ý của nạn nhân.
- Mã độc hại còn được định nghĩa là “một chương trình (program) được chèn một cách bí mật vào hệ thống với mục đích làm tổn hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống”
- Mã độc mang ý nghĩa rộng hơn virus

Lịch sử phát triển mã độc

Năm	Tên mã độc	Hành vi và thiệt hại
1971	Creeper Virus	Khi máy tính bị lây nhiễm sẽ hiển thị trên màn hình dòng chữ “The creeper”. Mặc dù không gây ra thiệt hại gì nhưng Creeper đã dự báo về một tương lai mã độc có thể lây lan diện rộng. Reaper là phần mềm AV đầu tiên tạo ra để loại bỏ Creeper
1978	Animal	Đây là Trojan đầu tiên, không phá hủy hệ thống nhưng có thể tự lan truyền trên mạng.
1981	Elk Cloner	Lây truyền nhanh chóng trên các máy Apple II thông qua đĩa mềm và hiển thị một bài thơ ngắn để chế nhạo người dùng. Được viết bởi một cậu bé 15 tuổi.
1983	Virus	Thuật ngữ virus lần đầu tiên được sử dụng để mô tả một chương trình máy tính trong một cuốn tiểu thuyết của Frederick Cohen
1986	Brain	Được phát minh bởi 2 anh em người Pakistan (17 tuổi và 24 tuổi). Mục đích để trùng phai và theo dõi những máy tính nào đã ăn cắp bản quyền phần mềm y tế viết cho máy tính IBM của họ.
1987	Jerusalem	Được thiết kế để phá hủy các tệp tin vào lõi lần xuất hiện của Thứ Sáu, ngày 13. Là một trong những virus phá hoại nhiều máy tính nhất (hoạt động 8 năm)

Lịch sử phát triển mã độc

Năm	Tên mã độc	Hành vi và thiệt hại
1988	Morris Worm	Là sâu máy tính đầu tiên, gây ra tấn công DDOS đầu tiên. Lợi dụng các thiết bị kết nối Internet, liên tục gửi các tập tin và lưu lượng đến cùng một địa chỉ IP, gây quá tải, và sập và hoàn toàn mất kết nối (hàng nghìn máy tính bị lây nhiễm)
1992	Michelangelo	Hàng ngàn máy tính chạy MS-DOS ngừng hoạt động vì một loại virus tự động kích hoạt vào đúng ngày sinh nhật của nhà điêu khắc lừng danh Michelangelo - 6/3
1999	Happy99, Melissa, Kak	Những mã độc này lây lan rất nhanh thông qua môi trường Microsoft bởi người dùng Internet
2000	ILOVEYOU	Là một loại sâu đã lây nhiễm thông qua 1 email, sau 10 ngày phát hành thiệt hại 50tr máy tính Windows. Thiệt hại lên tới 10 tỷ \$ → Đại dịch virus toàn cầu.
2000	Yahoo.com	Thông qua tấn công DDOS, một cậu bé 15 tuổi người Canada đã đánh sập Yahoo.com
2001	Nimda	Lây lan qua email, bằng cách tìm kiếm các địa chỉ email trong những file .html, mặt khác chúng lấy địa chỉ email thông qua giả mạo bằng dịch vụ MAPI. Gây thiệt hại lên tới 530tr trong tuần đầu tiên.

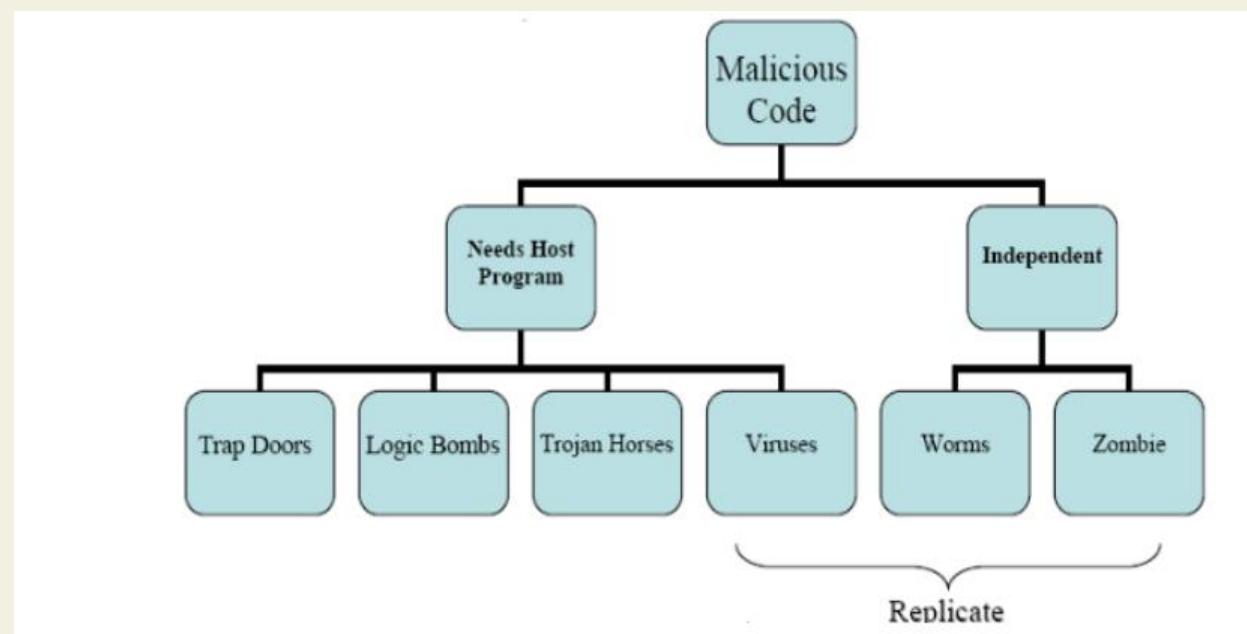
Lịch sử phát triển của mã độc

Năm	Tên mã độc	Hành vi và thiệt hại
2004	Santy	Là “webworm” đầu tiên, có khả năng lây lan mạnh, lây nhiễm vào các máy chủ Web đặt các diễn đàn trực tuyến viết bằng ngôn ngữ PHP, đồng thời SD goolge để tìm ra những máy chủ có lỗ hổng để lây nhiễm.
2007		Tấn công DDoS có chủ ý, làm sập trang web của thủ tướng cũng như một số tổ chức do chính phủ điều hành như trường học và ngân hàng
2008	Conficker	Đã lây nhiễm khoảng 10 triệu hệ thống máy chủ của Microsoft, bao gồm cả máy chính phủ và quân đội → An ninh mạng trong ý thức cộng đồng tăng lên
2010	Stuxnet	Nhắm vào các cơ sở hạt nhân của Iran. Được coi là dạng phần mềm độc hại tiên tiến nhất từng tạo ra. Khoảng 60 nghìn máy tính bị nhiễm trong đó 60% là ở Iran. Khoảng 5000 máy ly tâm của Iran đã “hóa điên” và kéo lùi dự án hạt nhân của Iran trong 2 năm.
2017	WannaCry	Tội phạm mạng đã sử dụng chính những tool của NSA để phát tán và lây lan mã độc. Nó mã hóa tập tin và người dùng phải trả 1 khoản tiền (BTC ~ 300usd) cho hacker. Gây ảnh hưởng hàng triệu users, 150 quốc gia, hơn 200 nhignf hệ thống mạng bị ảnh hưởng trong đó có VN.

Malware

Phân loại mã độc

- Theo hình thức lây nhiễm



Malware

Phân loại mã độc

- **Phân loại của NIST**
- **Virus** : là một loại mã độc hại (Malicious code) có khả năng tự nhân bản và lây nhiễm chính nó vào các file, chương trình hoặc máy tính
- **Worm**: là một chương trình có khả năng tự nhân bản và tự lây nhiễm trong hệ thống tuy nhiên nó có khả năng “tự đóng gói”, điều đó có nghĩa là Worm không cần phải có “file chủ” để mang nó khi nhiễm vào hệ thống
- **Trojan Horse**: Là loại mã độc hại được đặt theo sự tích “Ngựa thành Troy”. Trojan horse không tự nhân bản tuy nhiên nó lây vào hệ thống với biểu hiện rất ôn hòa nhưng thực chất bên trong có ẩn chứa các đoạn mã với mục đích gây hại
-

Malware

Phân loại mã độc

- **Malicious Mobile Code:** Là một dạng mã phần mềm có thể được gửi từ xa vào để chạy trên một hệ thống mà không cần đến lời gọi thực hiện của người dùng hệ thống. Malicious Mobile Code được coi là khác với virus, worm ở đặc tính là nó không nhiễm vào file và không tìm cách tự phát tán
- **Tracking Cookie:** Là một dạng lạm dụng cookie để theo dõi một số hành động duyệt web của người sử dụng một cách bất hợp pháp
- **Phần mềm gián điệp (Spyware):** Là loại phần mềm chuyên thu thập các thông tin từ các máy chủ (thông thường vì mục đích thương mại) qua mạng Internet mà không có sự nhận biết và cho phép của chủ máy

•

Malware

Phân loại mã độc

- **Phần mềm quảng cáo (Adware)**: rất hay có ở trong các chương trình cài đặt tải từ trên mạng. Một số phần mềm vô hại, nhưng một số có khả năng hiển thị thông tin lên màn hình, cưỡng chế người sử dụng.
- **Attacker Tool**: Là những bộ công cụ tấn công có thể sử dụng để đẩy các phần mềm độc hại vào trong hệ thống. Các bộ công cụ này có khả năng giúp cho kẻ tấn công có thể truy nhập bất hợp pháp vào hệ thống hoặc làm cho hệ thống bị lây nhiễm mã độc hại
- **Phishing**: Là một hình thức tấn công thường có thể xem là kết hợp với mã độc hại. Phishing là phương thức dụ người dùng kết nối và sử dụng một hệ thống máy tính giả mạo nhằm làm cho người dùng tiết lộ các thông tin bí mật về danh tính (ví dụ như mật khẩu, số tài khoản, thông tin cá nhân...)

•

Một số loại mã độc tiêu biểu

Mustang panda

- Mustang panda là nhóm tin tặc hoạt động từ năm 2014, có trụ sở hoạt động tại Trung Quốc, thường sử dụng các dòng mã độc PlugX, Cobalt Strike. Là nhóm tấn công APT có động cơ cao, được hậu thuẫn, kĩ thuật tinh vi để lây nhiễm và cài cắm mã độc với mục tiêu có được quyền truy cập vào máy nạn nhân để từ đó thực hiện hoạt động gián điệp và đánh cắp thông tin.
- Quốc gia mục tiêu: Úc, Bangladesh, Bỉ, Trung Quốc, Ethiopia, Đức, Hồng Kông, Ấn Độ, Mông Cổ, Myanmar, Nepal, Pakistan, Singapore, Hàn Quốc, Đài Loan, Anh, Mỹ, Việt Nam và LHQ.
- Các lĩnh vực mục tiêu: Hàng không, Chính phủ, Tổ chức phi chính phủ, Viễn thông

Một số loại mã độc tiêu biểu

Mustang panda

- *Các cuộc tấn công*

TT	Thời gian	Chiến dịch
1	8/2019	Anomanil Threat Research Team đã phát hiện ra các file .lnk đáng ngờ trong quá trình thu thập thông tin tình báo thường xuyên. Với phương pháp spear phishing có liên quan đến nhóm Mustang Panda.
2	01/2020	Các nhà bảo mật của hãng Avira phát hiện một phiên bản PlugX mới từ Mustang Panda APT, được sử dụng để do thám mục tiêu tại Hồng Kông và Việt Nam.
3	03/2020	Công ty an ninh mạng Việt Nam VinCSS phát hiện nhóm Mustang Panda phát tán email có đính kèm file .rar với mục đích giả mạo chỉ thị của Thủ tướng Việt Nam về đợt bùng phát Covid
4	03/2020	ATR xác định nhóm Mustang Panda đang sử dụng các lừa đảo theo chủ đề liên quan đến Corona virus.
5	03/2020	Anomali – Mustang tiến hành chiến dịch lợi dụng Covid-19 để tấn công vào Đài Loan

Một số loại mã độc tiêu biểu

Mustang panda

6	05/2020	Lab52 - Chiến dịch Dll-Sideload trojan với máy chủ C&C tạm thời
7	09/2020	Proofpoint – Chiến dịch tấn công Vaticant và các nhóm ngoại giao mục tiêu sử dụng biến thể viết bằng Golang mới của loader PlugX
8	03/2021	McAfee – Chiến dịch tấn công vào các hãng viễn thông nhằm đánh cắp bí mật 5G.
9	09/2021	Insikt Group – phát hiện Mustang tấn công vào các cơ quan chính phủ Indonesia.
10	02/2022	TalosIntelligence – Phát hiện chiến dịch tấn công vào các nước Châu Âu và Nga.

Một số loại mã độc tiêu biểu

Mã độc WannaCry

- Còn được biết đến với các tên khác như: WannaCrypt, WannaCrypt0r, WCRY là loại mã độc đặc biệt nguy hiểm, Ngoài việc mã hóa dữ liệu người dùng, còn lợi dụng lỗ hổng trên hệ điều hành windows để lây nhiễm cho các thiết bị khác đồng thời cài đặt cửa hậu trên máy tính bị nhiễm
- WannaCry đã taansc ông hơn 512000 thiết bị trên toàn thế giới. Nạn nhân sẽ phải trả một khoản tiền chuộc ít nhất 300 \$ (qua bitcoin) để lấy lại dữ liệu của mình, số tiền này sẽ tăng lên gấp đôi sau thời hạn 3 ngày, và sẽ bị mất sau 7 ngày nếu người dùng không thanh toán
- Chỉ sau 2 ngày được phát hiện, gây ảnh hưởng 10.000 tổ chức, 200.000 cá nhân trên 150 quốc gia.
- Được coi là mã độc nguy hiểm nhất thế giới,



Xuất hiện vào tháng 05/2017

Malware

Các kĩ thuật lây nhiễm và phá hoại trong Malware

- **Lây lan qua USB:** tạo ra một tệp autorun.inf trong thư mục gốc của USB. Khi phát hiện có thiết bị lưu trữ mới được cắm vào (USB, CD, Floppy Disk...), Window mặc nhiên sẽ kiểm tra tệp autorun.inf nằm trong đó, nếu có nó sẽ tự động thực hiện các dòng lệnh theo cấu trúc được sắp xếp trước
- **Lây lan qua Yahoo!Messenger:** tin nhắn rất hấp dẫn của bạn bè gửi cho và sau đó là đường link đến một trang web lạ, Virus đã được tự động down về máy và kích hoạt
- **Lây lan qua trình duyệt truy cập web:** thông qua đường link (một trang web bị nhiễm mã độc (dạng VBScript
- **Lây lan qua Email, Outlook Express:** "giả dạng" một e mail với một địa chỉ bất kì nào có nội dung là một tệp thiệp, một file attach hay đường link có chứa file malware gây nguy hiểm cho máy tính

Malware

Các kĩ thuật lây nhiễm và phá hoại trong Malware

- **Lây lan vào các tệp tin thực thi:** các file thực thi EXE, phổ biến cho các hệ thống Windows
- **Chia sẻ file**
- **Lỗ hổng của hệ điều hành hoặc ứng dụng**

Ảnh hưởng và tác hại của mã độc

Hệ thống file

- Nhân bản mã độc, lây nhiễm vào file
- Giấu trong những thư mục hệ thống
- Thiết lập thuộc tính ẩn, hệ thống để gây khó khăn trong việc tìm diệt
- Ẩn trong hệ thống file NTFS

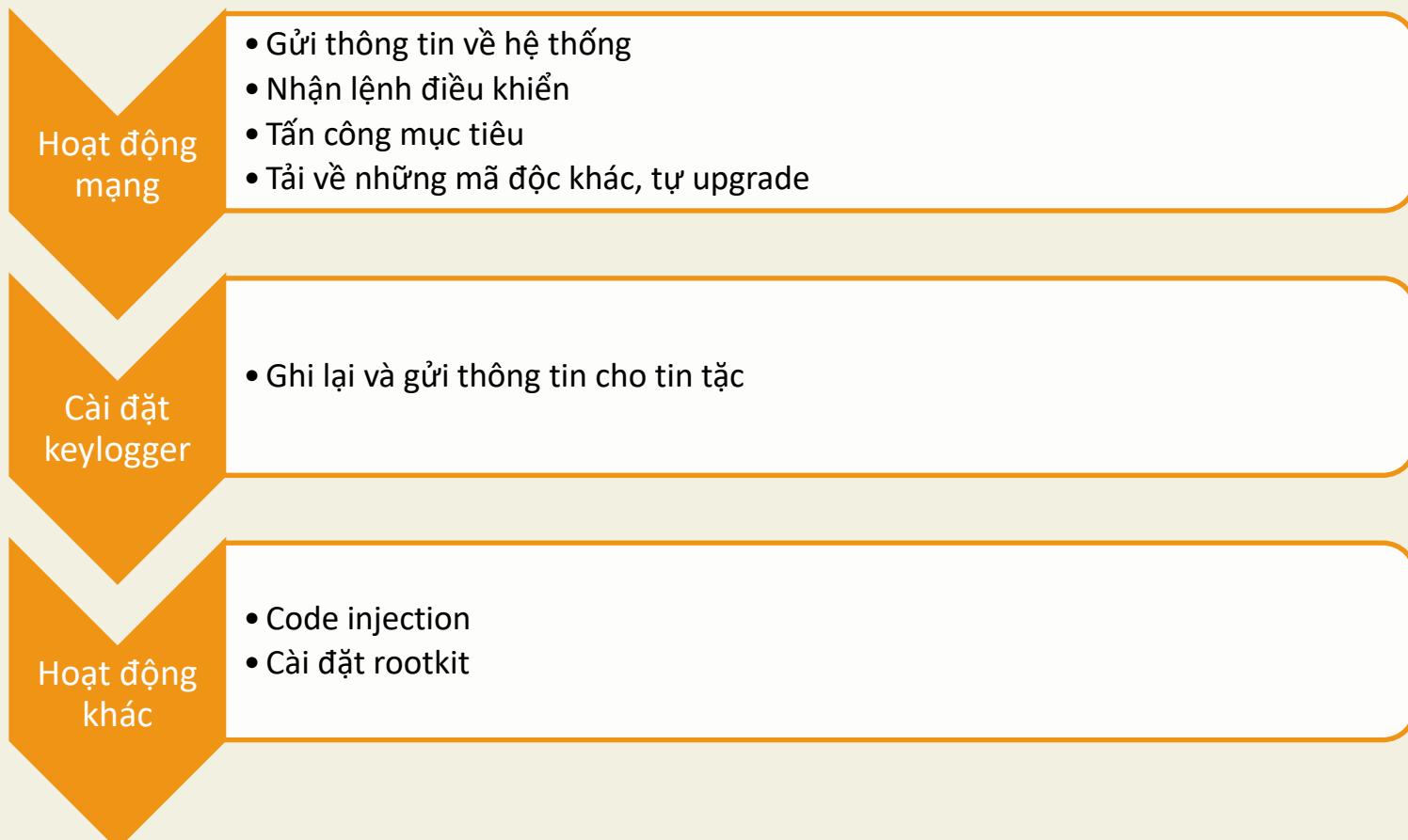
Registry

- Tạo những khóa mới để lưu giữ thông tin
- Thay đổi những giá trị của hệ thống
- Đọc những thuộc tính thông tin quan trọng
- Thường dùng để thiết lập chạy khi khởi động

Tiến trình

- Khởi tạo một tiến trình mới
- Khởi tạo một dịch vụ mới hoặc thay thế một dịch vụ đang hoạt động Malware DLL
- Kiểm tra những tiến trình đang chạy để tránh bị phát hiện
- Tự gắn vào những tiến trình hệ thống để tránh bị gỡ bỏ

Ảnh hưởng và tác hại của mã độc



Các phương pháp phát hiện mã độc

- Có 3 kỹ thuật nhận dạng đã được áp dụng:
 - dựa vào chuỗi nhận dạng (signaturebased approach),
 - dựa vào hành vi nghi ngờ (suspicious behavior-based approach)
 - dựa vào ý định (intention-based approach)

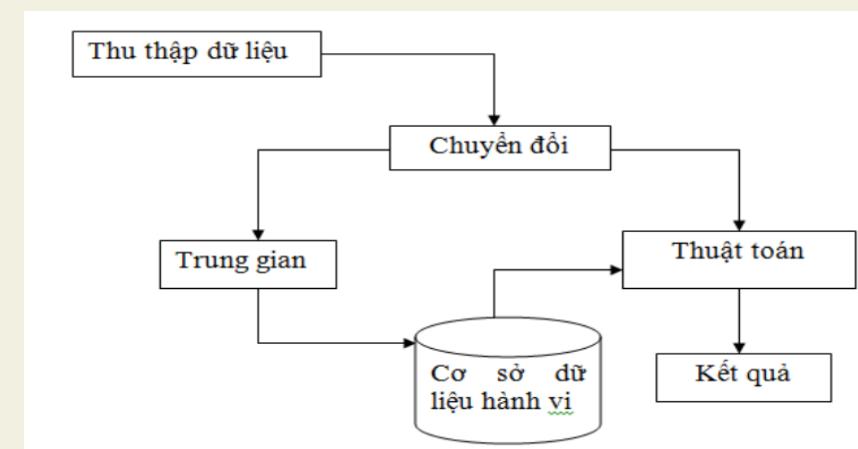
Các phương pháp phát hiện mã độc

- *Phương pháp phát hiện dựa vào chuỗi nhận dạng:*
- Hoạt động theo nguyên lý nhận dạng mẫu, các AV sử dụng một CSDL chứa mẫu virus (ID-virus library). Mỗi khi có virus mới, các chuyên gia anti-virus sẽ giải mã, trích chọn và cập nhật chuỗi nhận dạng virus vào thư viện. Thông tin về đối tượng chẩn đoán (ghi nhận từ hệ thống đích) cùng với thông tin của virus (trong thư viện mẫu) sẽ cho kết luận về tình trạng của đối tượng
- Nhận dạng mẫu giúp AV phát hiện các virus đã biết trên tập dữ liệu chẩn đoán với độ chính xác cao
- Nhược điểm: Cồng kềnh, Bị động, Nhầm lẫn

Malware

Các phương pháp phát hiện mã độc

- *Phương pháp phát hiện dựa trên hành vi*
- xác định các hành động thực hiện của mã độc hơn là việc xác định cấu trúc nhị phân của chương trình. Các chương trình không giống với cú pháp hay cấu trúc nhưng có hành vi giống với những hành vi đã xác định trước là đã xác định được nó là mã độc hay không



Các phương pháp phát hiện mã độc

Malware

- *Phát hiện virus dựa vào ý định :*
- Những thay đổi quan trọng trong tập tin, cấu hình hệ thống hay HĐH đều được cảnh báo như một mối hiểm họa tiềm tàng
- Mặc dù đơn giản nhưng tiếp cận này tỏ ra khá hiệu quả vì nó có thể bảo vệ máy tính khỏi các mối đe dọa chưa được biết đến, kể cả virus máy tính

Phân tích mã độc

• Phân tích mã độc để làm gì?

Phân tích mã độc là thực hiện các biện pháp nghiệp vụ để thu thập, tìm hiểu, nghiên cứu mọi thông tin về mã độc

- ✓ Hành vi của mã độc
- ✓ Ảnh hưởng, tác hại

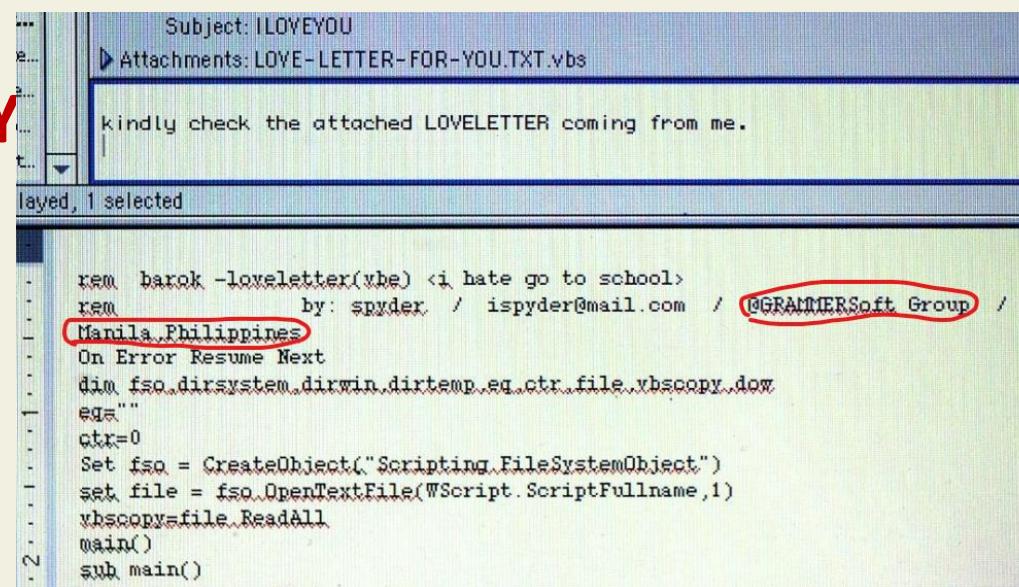


- Cảnh báo
 - Biện pháp phòng chống, ngăn chặn
-
- ✓ Lây lan của mã độc
 - ✓ Lỗ hỏng bị khai thác

Phân tích mã độc

- Phân tích mã độc để làm gì?

Ví dụ: ILOVEY



```
Subject: ILOVEYOU
> Attachments: LOVE-LETTER-FOR-YOU.TXT.vbs

kindly check the attached LOVELETTER coming from me.

1 selected

rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / MGRAMMERSoft Group /
Manila, Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eg,ctr,file,vbscopy,dow
eg=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
2
```

- Phương pháp phân tích mã độc

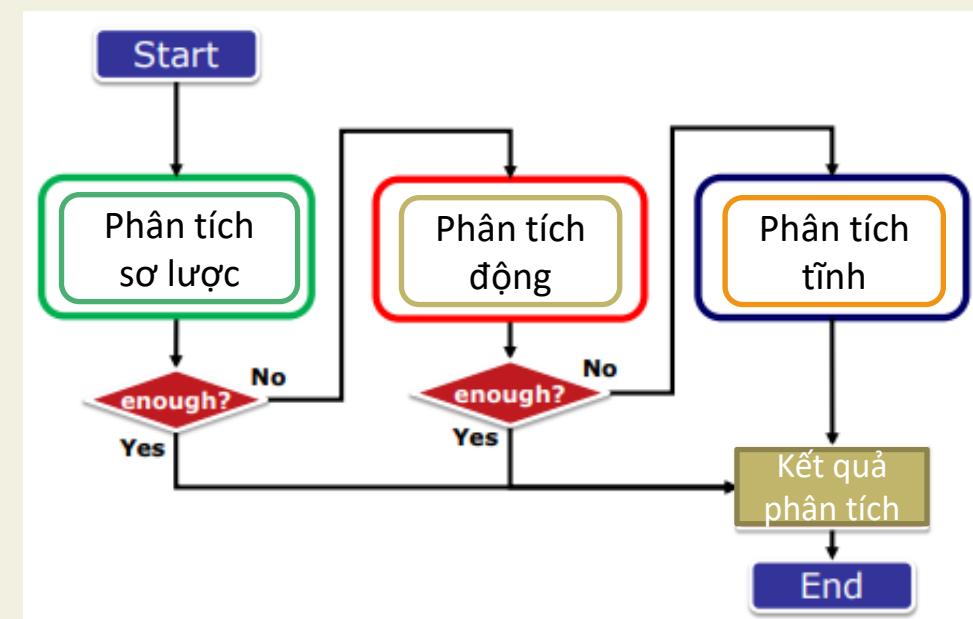


Phân tích mã độc

	Phân tích sơ lược	Phân tích động	Phân tích tĩnh
Tổng quan	Thu thập thông tin từ đối tượng bị tấn công mà không cần thực thi mã độc	Thực thi mã độc và giám sát hành vi	Đọc code – dịch ngược và hiểu các chức năng của mã độc
Đầu ra	<ul style="list-style-type: none"> - Hàm băm - Strings - Các thuộc tính file - Thông tin đóng gói - Thông tin từ các AV 	<p>Hoạt động:</p> <ul style="list-style-type: none"> - File system - Registry - Process - Network 	<p>Các chức năng của mã độc.</p> <p>Ví dụ:</p> <ul style="list-style-type: none"> - Bot commands - Encode/Decode methods
Nguy cơ an toàn	Thấp	Cao	Trung bình
Hiệu quả phân tích	Thấp	Trung bình	Cao

Giới thiệu về phân tích mã độc

• Sơ đồ các bước phân tích mã độc



Giới thiệu về phân tích mã độc

Một số điểm lưu ý khi phân tích mã độc

❖ Thận trọng khi phân tích

- *Một sai lầm có thể dẫn tới hậu quả nghiêm trọng*

❖ Cân nhắc khi công bố kết quả

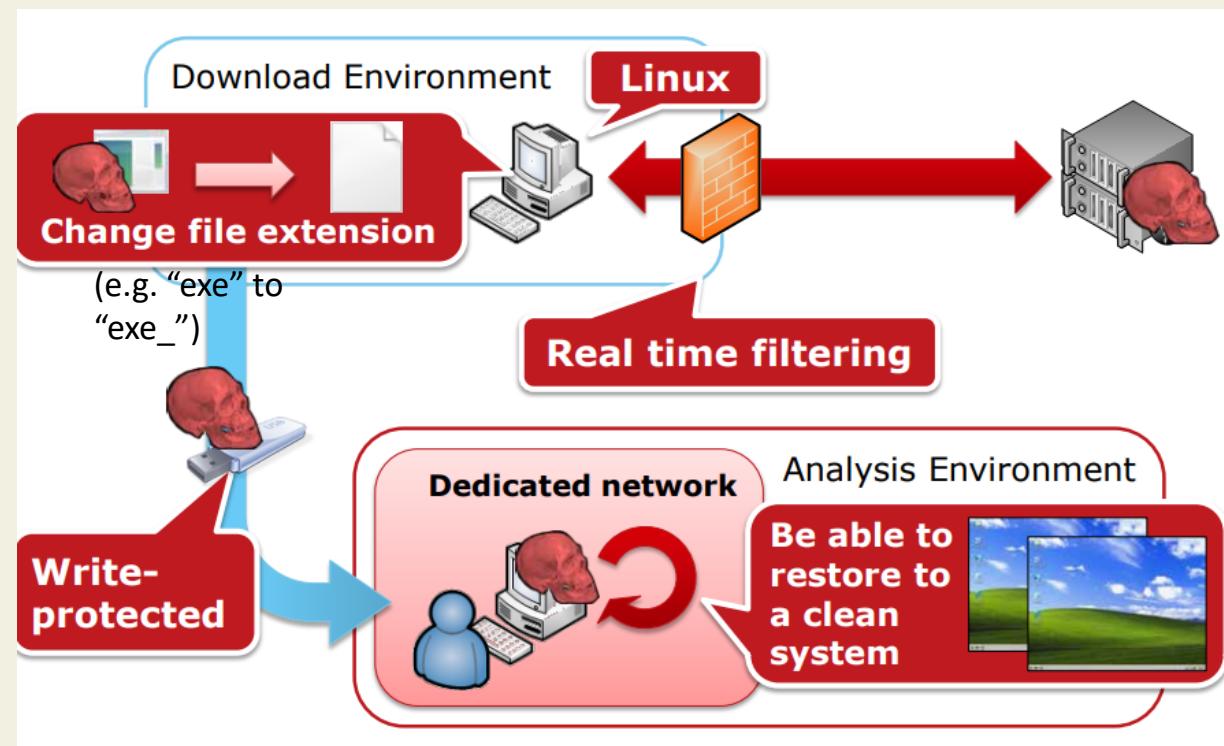
Kết quả phân tích chi tiết được công bố có thể dẫn tới xuất hiện những mã độc mạnh hơn

❖ Xây dựng môi trường phân tích an toàn

- *Chú ý tới môi trường để tải về mã độc, phân tích mã độc và kết quả phân tích*

Phân tích mã độc

- Môi trường phân tích an toàn



Câu hỏi:

- Câu 1: Tìm hiểu ít nhất 5 loại mã độc nguy hiểm trên thế giới? (Tên mã độc, tổ chức/cá nhân phát tán/tạo, mức thiệt hại bao nhiêu, số lượng máy tính, quốc gia bị nhiễm, cơ chế lây nhiễm, ...)
- Câu 2: Kể tên các tổ chức, doanh nghiệp tại Việt Nam có job về phân tích mã độc?

PHÁT HIỆN XÂM NHẬP VÀ TƯỜNG LỬA

Một số khái niệm về xâm nhập (Intrusion)

Có 3 đối tượng xâm nhập (intruder) cơ bản:

- ***Masquerader***: Một cá nhân không được phép sử dụng máy tính và xâm nhập vào các biện pháp kiểm soát truy cập của hệ thống để khai thác tài khoản của người dùng hợp pháp.
- ***Misfeasor***: người dùng được chứng thực để sử dụng các tài nguyên hệ thống nhưng sử dụng sai quyền truy cập của mình trên hệ thống.
- ***Clandestine user***: có thể được định nghĩa là một cá nhân chiếm hệ thống kiểm soát của hệ thống và vượt qua hệ thống bảo mật của hệ thống.

Một số ví dụ về xâm nhập hệ thống:

- Thực hiện xâm nhập root từ xa của máy chủ e-mail
- Thay đổi giao diện máy chủ Web
- Đoán và bẻ khóa mật khẩu
- Sao chép cơ sở dữ liệu chứa số thẻ tín dụng
- Xem dữ liệu nhạy cảm, bao gồm hồ sơ bảng lương và thông tin y tế mà không được phép
- Chạy trình nghe gói tin trên máy trạm để lấy tên người dùng và mật khẩu
- Sử dụng lỗi cấp phép trên máy chủ FTP ẩn danh để phân phối phần mềm và tệp nhạc vi phạm bản quyền
- Quay số vào modem không bảo mật và truy cập mạng nội bộ
- Đóng vai người điều hành, gọi đến bộ phận trợ giúp, đặt lại mật khẩu e-mail của người điều hành và tìm hiểu mật khẩu mới
- Sử dụng máy trạm đã đăng nhập, không được giám sát mà không được phép

Các dạng hành vi xâm nhập:

- HACKER (TIN TẮC): Theo truyền thống, những kẻ xâm nhập vào máy tính làm vậy vì cảm giác phấn khích hoặc vì địa vị trong giới. Hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS) được thiết kế để chống lại loại mối đe dọa từ hacker này.
- TỘI PHẠM: Các nhóm tin tặc có tổ chức đã trở thành mối đe dọa phổ biến và phổ biến đối với các hệ thống trên Internet. IDS và IPS cũng có thể được sử dụng cho những loại kẻ tấn công này, nhưng có thể kém hiệu quả hơn do tính chất ra vào nhanh chóng của cuộc tấn công.
- TẤN CÔNG NỘI BỘ: Các cuộc tấn công nội bộ là một trong những loại tấn công khó phát hiện và ngăn chặn nhất.

Các kỹ thuật xâm nhập:

- Mục tiêu của kẻ xâm nhập là giành quyền truy cập vào hệ thống hoặc tăng phạm vi đặc quyền có thể truy cập được trên hệ thống. Hầu hết các cuộc tấn công ban đầu đều sử dụng các lỗ hổng hệ thống hoặc phần mềm cho phép người dùng thực thi mã mở cửa sau vào hệ thống.
- Ngoài ra, kẻ xâm nhập cố gắng lấy thông tin đáng lẽ phải được bảo vệ. Trong một số trường hợp, thông tin này ở dạng **mật khẩu người dùng**. Với kiến thức về mật khẩu của một số người dùng khác, kẻ xâm nhập có thể đăng nhập vào hệ thống và thực hiện tất cả các đặc quyền dành cho người dùng hợp pháp.

Dữ liệu mật khẩu có thể được bảo vệ theo 2 cách:

- ✓ Hàm một chiều one-way function
- ✓ Kiểm soát truy cập

• Các kỹ thuật xâm nhập:

Để vượt qua cơ chế bảo vệ dữ liệu mật khẩu, thì attacker phải nỗ lực để tìm hiểu mật khẩu. Một số kỹ thuật để bẻ khóa mật khẩu như sau:

1. Thử mật khẩu mặc định được sử dụng với các tài khoản tiêu chuẩn đi kèm với hệ thống. Nhiều quản trị viên không bận tâm đến việc thay đổi các giá trị mặc định này.

2. Hãy thử kỹ tất cả các

3. Thử các từ trong từ điển có sẵn trên bảng tin của

4. Thu thập thông tin về trong văn phòng của họ

5. Hãy thử số điện thoại, số An sinh xã hội và số phòng của người dùng.

6. Hãy thử tất cả các biển số xe hợp pháp của tiểu bang này.

7. Sử dụng mã độc Trojan để vượt qua các hạn chế truy cập.

8. Tấn công vào kết nối giữa người dùng từ xa và hệ thống máy chủ.

Phát hiện và phòng ngừa xâm nhập hệ thống như thế nào?

Các ví dụ về cái sau

họ, những bức ảnh

ch.

Phát hiện xâm nhập: Vì sao lại cần phát hiện xâm nhập?

1. Nếu phát hiện hành vi xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định và loại bỏ khỏi hệ thống trước khi xảy ra bất kỳ thiệt hại nào hoặc bất kỳ dữ liệu nào bị xâm phạm. Ngay cả khi việc phát hiện không đủ kịp thời để ngăn chặn kẻ xâm nhập thì việc phát hiện xâm nhập càng sớm thì mức độ thiệt hại càng ít và khả năng phục hồi càng nhanh.
2. Một hệ thống phát hiện xâm nhập hiệu quả có thể đóng vai trò ngăn chặn, do đó có tác dụng ngăn chặn các hành vi xâm nhập.
3. Phát hiện xâm nhập cho phép thu thập thông tin về các kỹ thuật xâm nhập có thể được sử dụng để tăng cường cơ sở ngăn chặn xâm nhập.

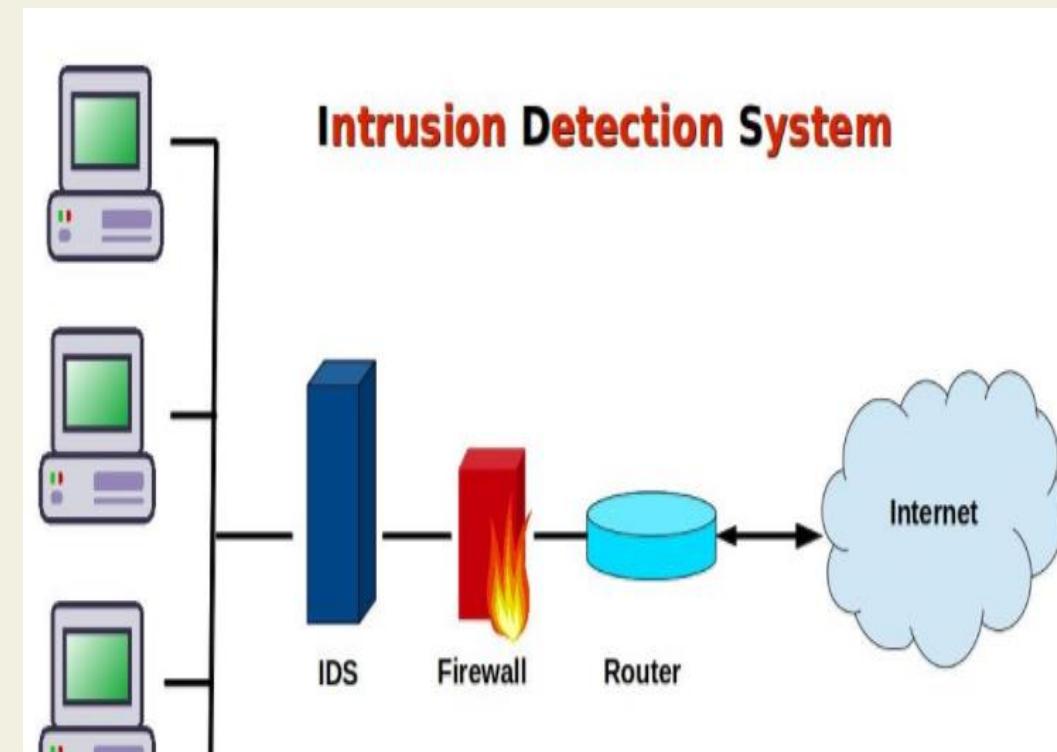
Các phương pháp phát hiện xâm nhập:

1. **Phát hiện sự bất thường về thống kê (Statistical anomaly detection)**: Liên quan đến việc thu thập dữ liệu về hành vi của người dùng hợp pháp trong một khoảng thời gian. Sau đó, các kiểm tra thống kê được áp dụng cho hành vi được quan sát để xác định với mức độ tin cậy cao xem hành vi đó có phải là hành vi hợp pháp của người dùng hay không.
 - a. **Phát hiện ngưỡng - Threshold detection**: Cách tiếp cận này liên quan đến việc xác định các ngưỡng, độc lập với người dùng, cho tần suất xuất hiện của các sự kiện khác nhau.
 - b. **Dựa trên hồ sơ - Profile-based**: Hồ sơ về hoạt động của mỗi người dùng được phát triển và sử dụng để phát hiện những thay đổi trong hành vi của từng tài khoản.
2. **Phát hiện dựa trên quy tắc (Rule-based detection)**: Liên quan đến nỗ lực xác định một bộ quy tắc hoặc kiểu tấn công có thể được sử dụng để quyết định rằng một hành vi nhất định là của kẻ xâm nhập. Điều này thường được gọi là phát hiện dựa vào chữ ký - signature detection.

Phát hiện xâm nhập

• Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System)

- ✓ IDS là một hệ thống phòng chống, nhằm phát hiện các hành động tấn công vào một mạng.
- ✓ Mục đích là phát hiện và ngăn ngừa các hành động phá hoại đối với vấn đề bảo mật hệ thống, hoặc những hành động trong tiến trình tấn công như quét các cổng.
- ✓ Một tính năng chính của hệ thống này là cung cấp thông tin nhận biết về những hành động không bình thường và đưa ra các thông báo cho quản trị viên mạng để khóa các kết nối đang tấn công.
- ✓ Thêm vào đó công cụ IDS cũng có thể phân biệt giữa những tấn công từ bên trong tổ chức và tấn công bên ngoài (tấn công từ hacker).



Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System)

- Khi một sự xâm nhập được phát hiện, IDS đưa ra các cảnh báo đến các quản trị viên hệ thống về sự việc này.
- Bước tiếp theo được thực hiện bởi các quản trị viên hoặc có thể là bản thân IDS



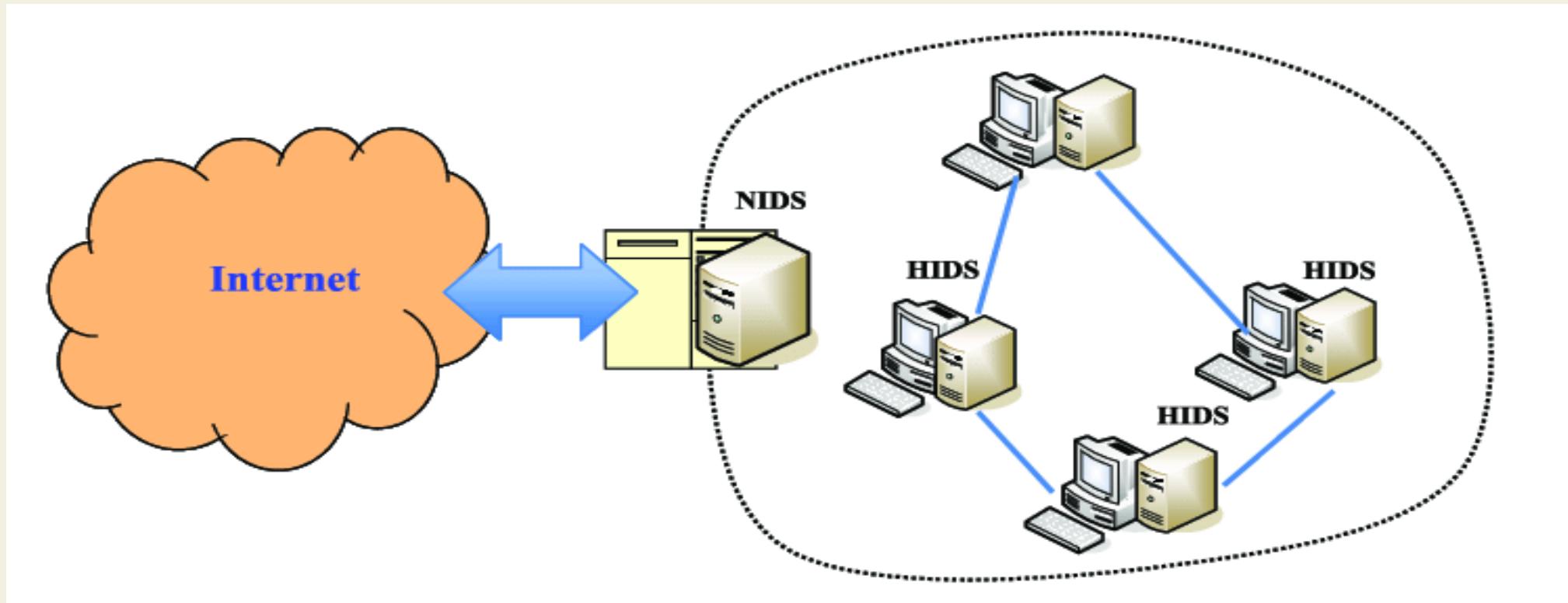
- Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System)

Phân loại IDS:

- Phân loại theo phạm vi giám sát:
 - ***Network-based IDS (NIDS)***: là những IDS giám sát trên toàn bộ mạng.
 - ***Host-based IDS (HIDS)***: là những IDS giám sát hoạt động của từng máy tính riêng biệt
- Phân loại theo kỹ thuật:
 - ***Signature-based IDS***: phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập, căn cứ trên nhật ký hoạt động của hệ thống.
 - ***Anomaly-based IDS***: phát hiện xâm nhập bằng cách so sánh (mang tính thống kê) các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường.

Phát hiện xâm nhập

- Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System)



Network-based IDS: được sử dụng để giám sát traffic đến và đi từ tất cả các thiết bị trên mạng

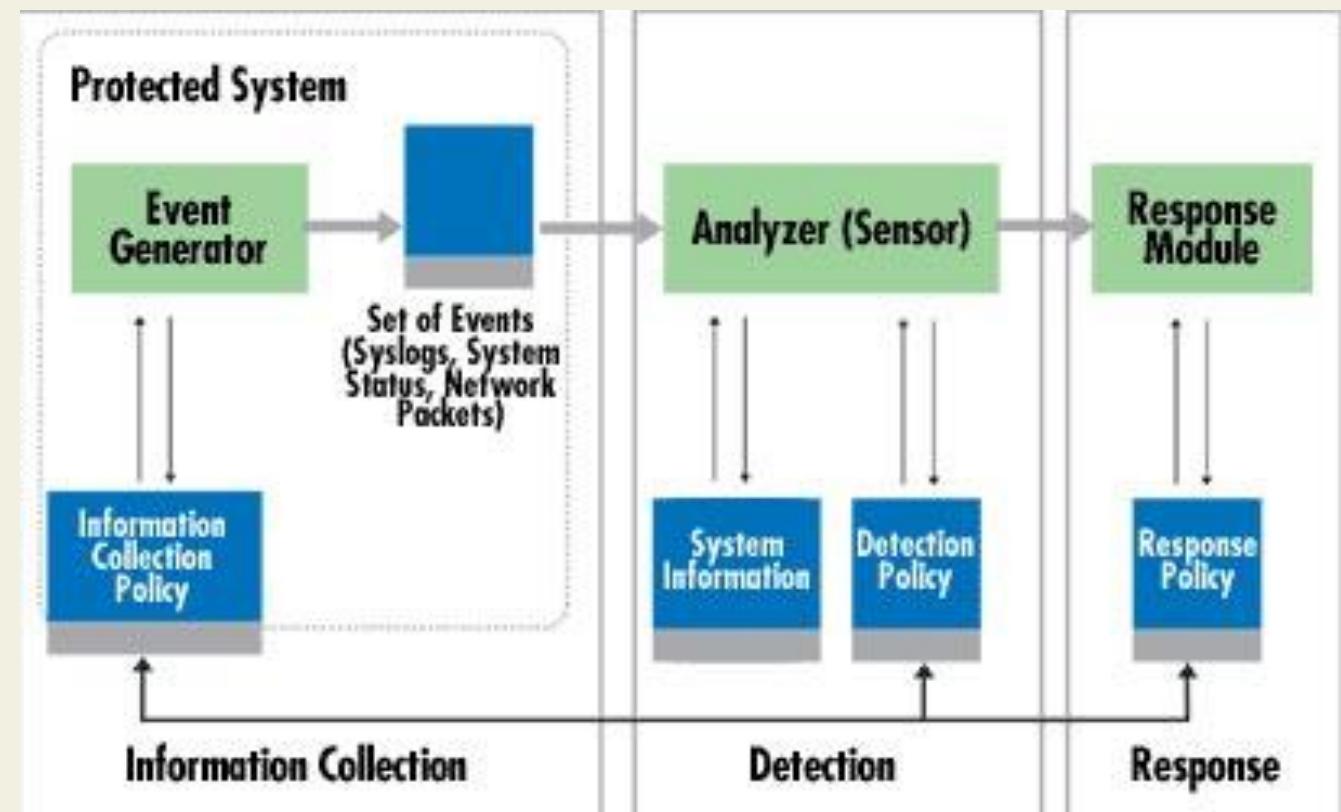
HIDS: cài đặt một phần mềm trên máy chủ, IDS dựa trên máy chủ quan sát tất cả những hoạt động về hệ thống và các file log, lưu lượng mạng thu thập, ...

Phát hiện xâm nhập

- Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System)

Cấu trúc gồm 3 thành phần chính:

- ✓ Thành phần thu thập gói tin (*information collection*);
- ✓ Thành phần phân tích gói tin (*Detection*);
- ✓ Thành phần phản hồi (*Response*) nếu gói tin đó được phát hiện là một cuộc tấn công.

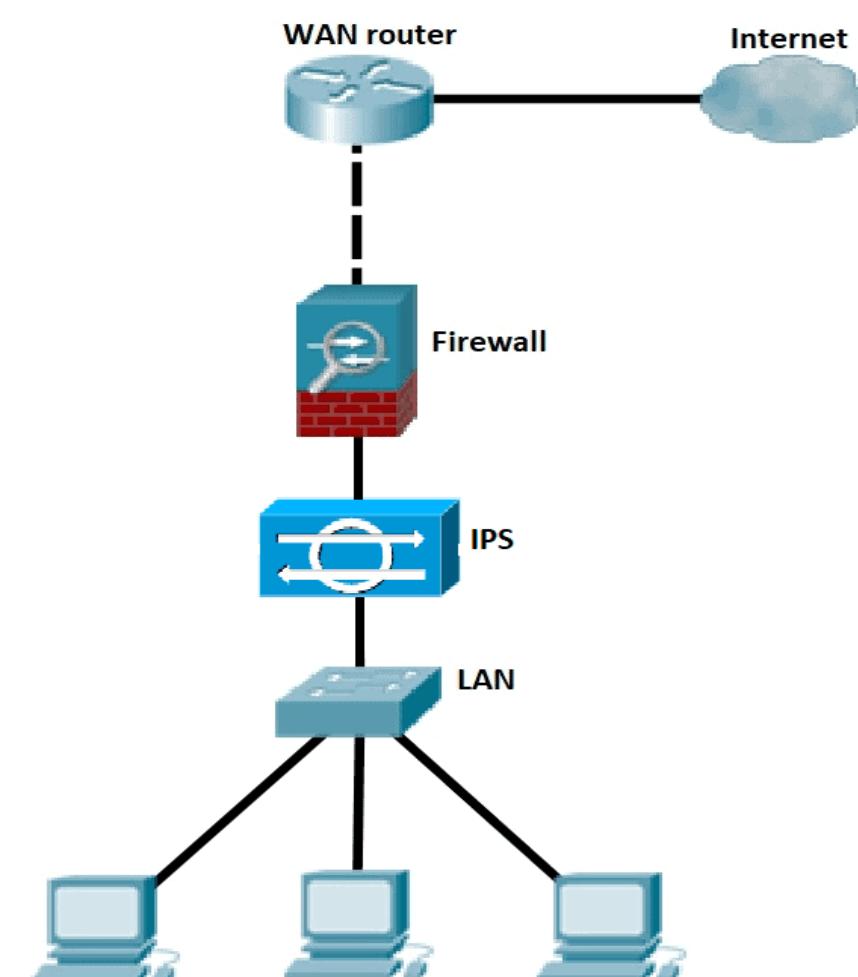


Phát hiện xâm nhập

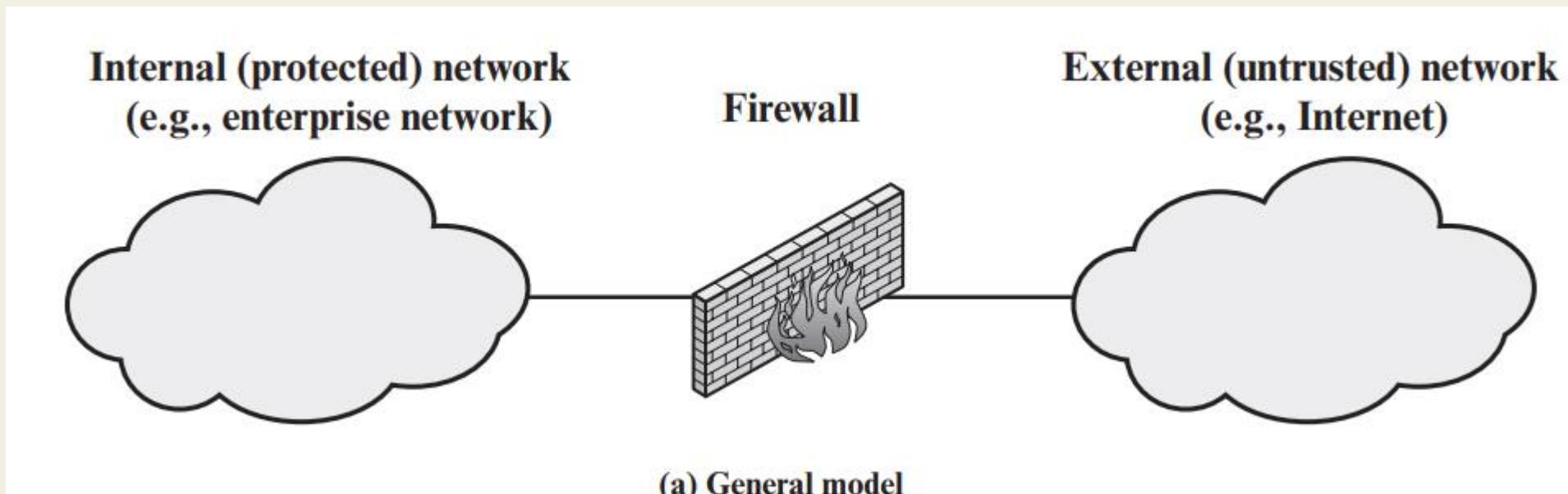
Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System)

- Nên triển khai IDS ở vị trí nào?

- Đặt giữa router và firewall
- Đặt trong miền DMZ
- Đặt sau firewall



- **Khái niệm:** Firewall là một công cụ phần cứng hoặc phần mềm hoặc cả 2 được tích hợp vào hệ thống để chống lại sự truy cập trái phép, ngăn chặn virus... để đảm bảo nguồn thông tin nội bộ được an toàn, tránh bị kẻ gian đánh cắp thông tin.
- Nói ngắn gọn và dễ hiểu hơn thì Firewall chính là ranh giới bảo mật giữa bên trong và bên ngoài của một hệ thống mạng máy tính.



- **Vai trò:** Firewall giúp kiểm soát luồng thông tin giữa Intranet và Internet, chúng phát hiện và phán xét những hành vi được truy cập và không được truy cập vào bên trong hệ thống, đảm bảo tối đa sự an toàn thông tin.

Tính năng chính của dòng thiết bị này có thể được tóm tắt ở những gạch đầu dòng dưới đây:

- Cho phép hoặc vô hiệu hóa các dịch vụ truy cập ra bên ngoài, đảm bảo thông tin chỉ có trong mạng nội bộ.
- Cho phép hoặc vô hiệu hóa các dịch vụ bên ngoài truy cập vào trong.
- Phát hiện và ngăn chặn các cuộc tấn công từ bên ngoài.
- Hỗ trợ kiểm soát địa chỉ truy cập (bạn có thể đặt lệnh cấm hoặc là cho phép).
- Kiểm soát truy cập của người dùng.
- Quản lý và kiểm soát luồng dữ liệu trên mạng.

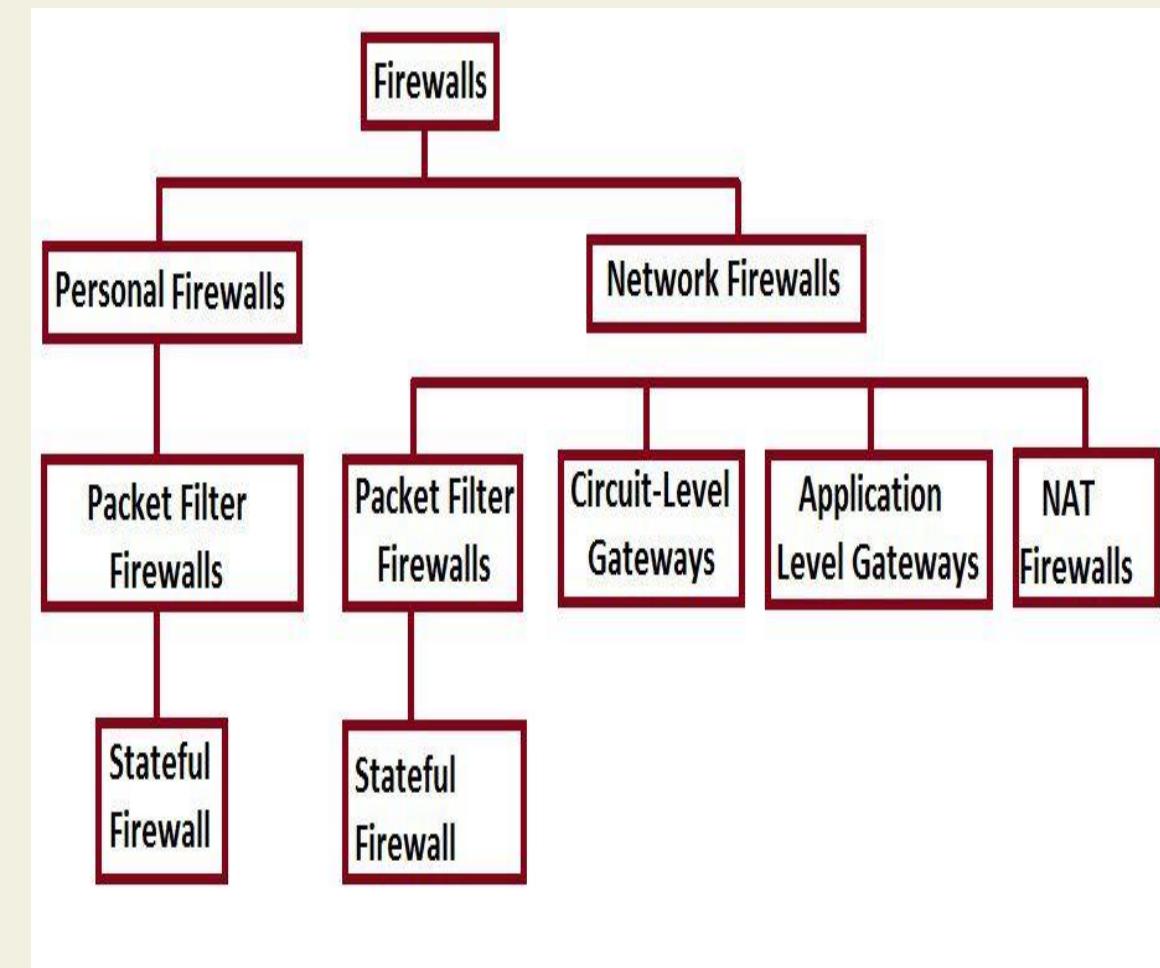
- **Vai trò:**

- Xác thực quyền truy cập.
- Hỗ trợ kiểm soát nội dung thông tin và gói tin lưu chuyển trên hệ thống mạng.
- Lọc các gói tin dựa vào địa chỉ nguồn, địa chỉ đích và số Port (hay còn gọi là cổng), giao thức mạng.
- Người quản trị có thể biết được kẻ nào đang cố gắng để truy cập vào hệ thống mạng.
- Firewall hoạt động như một Proxy trung gian.
- Bảo vệ tài nguyên của hệ thống bởi các mối đe dọa bảo mật.
- Cân bằng tải: Bạn có thể sử dụng nhiều đường truyền internet cùng một lúc, việc chia tải sẽ giúp đường truyền internet ổn định hơn rất nhiều.

- Phân loại

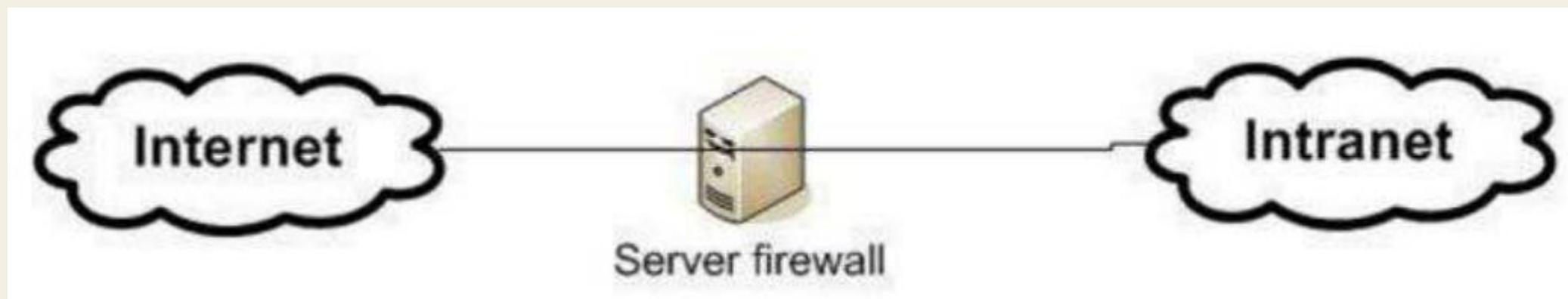
Personal Firewall: Loại này được thiết kế để bảo vệ một máy tính trước sự truy cập trái phép từ bên ngoài.

Network Firewalls: Được thiết kế ra để bảo vệ các host trong mạng trước sự tấn công từ bên ngoài.



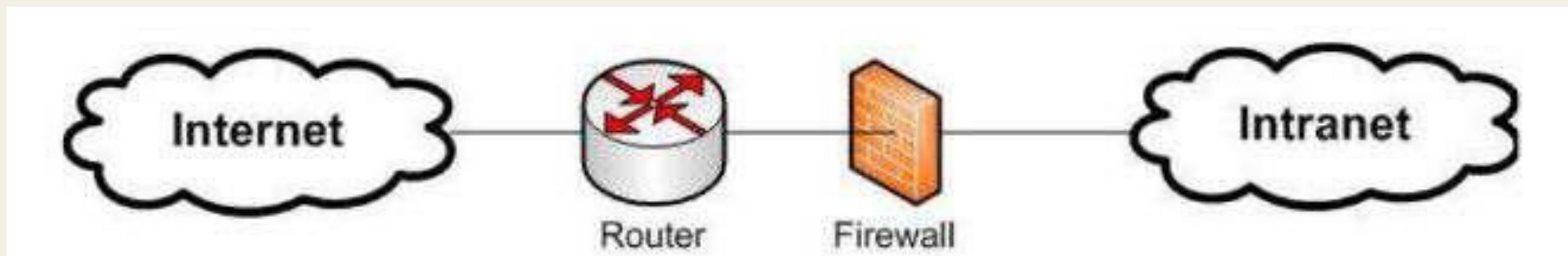
Sản phẩm Firewall được ứng dụng trong thực tế

- ***Software Firewalls***: Hay còn gọi là Firewall mềm, đây là loại Firewall được tích hợp trên hệ điều hành, nó bao gồm các sản phẩm như: SunScreen firewall, Check Point NG, IPF, Linux's IPTables, Microsoft ISA server ...



Sản phẩm Firewall được ứng dụng trong thực tế

- **Appliance Firewalls:** Hay còn gọi là Firewall cứng. Đây là loại Firewall cứng được tích hợp sẵn trên các phần cứng chuyên dụng, thiết kế này dành riêng cho Firewall. Một số Firewall cứng như Cisco PIX, WatchGuard Fireboxes, NetScreen firewall, SonicWall Appliances, Nokia firewall...



Ngoài ra còn có **Integrated firewalls**: Hay còn gọi là Firewall tích hợp. Ngoài chức năng cơ bản của Firewall ra thì nó còn đảm nhận các chức năng khác ví dụ như VPN, phát hiện và chống xâm nhập từ bên ngoài, lọc thư rác, chống lại virus...

Ôn tập