**CÂU HỎI CHƯƠNG 2**

**MỤC LỤC**

[Phần 1: Cryptography 3](#_Toc415236345)

[1) MD5 hay SHA có thể sử dụng để mã hóa thông điệp như email không? Tại sao? 3](#_Toc415236346)

[2) Cơ chế mã hóa Symmetric? 4](#_Toc415236347)

[3) Cơ chế mã hóa Asymmetric? 5](#_Toc415236348)

[4) Cơ chế mã hóa DES? Trình bày, giải thích các biện pháp nâng cao tính bảo mật DES? 6](#_Toc415236349)

[5) Cơ chế mã hóa nào được dùng để thay thế DES? Trình bày cơ chế đó. Các ưu điểm của cơ chế đó so với DES? 8](#_Toc415236350)

[6) Cách thức mã hóa RSA? 9](#_Toc415236351)

[Phần 2: Authentication 11](#_Toc415236352)

[1) Kĩ thuật nào giả dạng IP Source/Destination? 11](#_Toc415236353)

[2) Nêu đặc điểm, tính chất, cơ chế của các dạng tấn công mạng sau: spoofing, man-in-the-middle, playback, Hijacking. 11](#_Toc415236354)

[Phần 3: Integrity 13](#_Toc415236355)

[1) Hàm băm là gì? Có mấy loại hàm băm? Tính chất của hàm băm? 13](#_Toc415236356)

[2) Chữ ký số là gì? Các đặc điểm của chữ ký số? 14](#_Toc415236357)

[3) Hãy miêu tả cách thức hoạt động của việc xác nhận tính toàn vẹn nội dung của một message? 15](#_Toc415236358)

[Phần 4: Key Distribution & Certification 16](#_Toc415236359)

[1) KDC dùng để làm gì? Cơ chế hoạt động. 16](#_Toc415236360)

[2) CA Server dùng để làm gì? Cơ chế hoạt động. 17](#_Toc415236361)

[3) Nêu các tổ chức/cty cung cấp dịch vụ KDC, CA ở Việt Nam? 18](#_Toc415236362)

[4) Tác dụng của Certification là gì? Liệt kê các trường thông tin chính trong 1 certification. 19](#_Toc415236363)

[5) IPSec dùng cơ chế Symmetric hay Asymmetric Key? Thuật toán mã hóa của nó là gì? Mô tả cơ chế bảo mật của IPSec. 19](#_Toc415236364)

[Phần 5: Firewall 19](#_Toc415236365)

[1) Nhiệm vụ chung của Firewall? chức năng của Firewall trên môi trường mạng Internet? 19](#_Toc415236366)

[2) Có mấy loại Firewall theo cơ chế hoạt động? Chức năng cơ chế của mỗi loại. 21](#_Toc415236367)

[3) So sánh ưu và khuyết điểm của các loại Firewall? 24](#_Toc415236368)

[Phần 6: Attacks and Counter measures 25](#_Toc415236369)

[1) Tấn công dạng Mapping được dùng để làm gì? Cơ chế tấn công. Cách phòng chống. 25](#_Toc415236370)

[2) Packet sniffing được dùng để làm gì? Cơ chế tấn công. Cách phòng chống. 27](#_Toc415236371)

[3) Ip Spoofing được dùng để làm gì? Cơ chế tấn công. Cách phòng chống. 29](#_Toc415236372)

[4) Liệt kê một số giao thức, thuật toán nổi bật về Security ở từng OSI Layer. 34](#_Toc415236373)

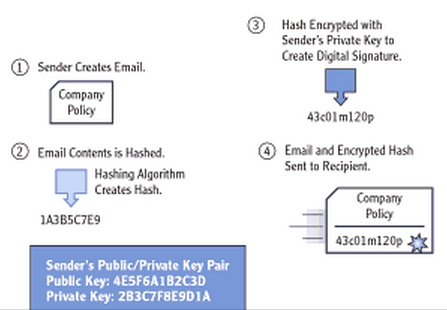
# Phần 1: Cryptography

## MD5 hay SHA có thể sử dụng để mã hóa thông điệp như email không? Tại sao?

MD5 hay SHA có thể sử dụng để mã hóa thông điệp như email. Vì:

* Một MD5 hash là một “hàm mã hóa”
* Nó sẽ lấy một mãnh tùy ý của dữ liệu, như một địa chỉ email và chuyển đổi nó thành một chuỗi gồm 32 ký tự.
* Mỗi khi bạn chạy cùng một mãnh của dữ liệu thông qua các thuật toán băm bạn nhận được kết quả tương tự.
* Điều đó có nghĩa là địa chỉ email của bạn “một giá trị duy nhất” được chuyển thành một chuỗi băm duy nhất thông qua quá trình này.

**Ví Dụ:**



Hình 1: Quá trình người gửi mã hóa email

1. Người gửi tạo email

Đối với ví dụ này, các email không cần phải được giữ bí mật. Nếu đang cần bảo mật, nó có thể được mã hóa. Tuy nhiên, ví dụ này chỉ tập trung vào các chữ ký số.

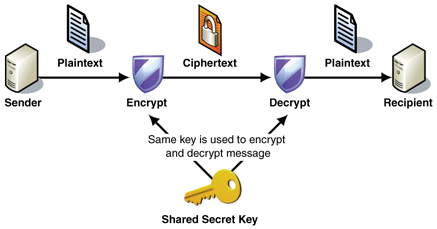
1. Các nội dung của email được băm

Trong ví dụ này, các hash là 1A3B5C7E9. Nếu đây là MD5, nó sẽ là 32 số thập lục phân; và nếu nó là SHA-1, nó sẽ là 40 số thập lục phân.

1. Các hash của các email được mã hóa bằng khóa riêng của người gửi.

Trong ví dụ này, điều này sẽ cho một kết quả là 43c01m120p.

## Cơ chế mã hóa Symmetric?



Hình 2: Mã hóa đối xứng (Symmetric)

Trong hệ thống mã hoá đối xứng, trước khi truyền dữ liệu, 2 bên gửi và nhận phải thoả thuận về khoá dùng chung cho quá trình mã hoá và giải mã. Sau đó, bên gửi sẽ mã hoá bản rõ (Plaintext) bằng cách sử dụng khoá bí mật này và gửi thông điệp đã mã hoá cho bên nhận. Bên nhận sau khi nhận được thông điệp đã mã hoá sẽ sử dụng chính khoá bí mật mà hai bên thoả thuận để giải mã và lấy lại bản rõ (Plaintext).

Hình vẽ trên chính là quá trình tiến hành trao đổi thông tin giữa bên gửi và bên nhận thông qua việc sử dụng phương pháp mã hoá đối xứng. Trong quá trình này, thì thành phần quan trọng nhất cần phải được giữ bí mật chính là khoá. Việc trao đổi, thoả thuận về thuật toán được sử dụng trong việc mã hoá có thể tiến hành một cách công khai, nhưng bước thoả thuận về khoá trong việc mã hoá và giải mã phải tiến hành bí mật.

## Cơ chế mã hóa Asymmetric?



Hình 3: Mã hóa bất đối xứng (Asymmetric)

Quá trình truyền và sử dụng mã hoá khoá công khai được thực hiện như sau:

* Bên gửi yêu cầu cung cấp hoặc tự tìm khoá công khai của bên nhận trên một server chịu trách nhiệm quản lý khoá.
* Sau đó hai bên thống nhất thuật toán dùng để mã hoá dữ liệu, bên gửi sử dụng khoá công khai của bên nhận cùng với thuật toán đã thống nhất để mã hoá thông tin được gửi đi.
* Khi nhận được thông tin đã mã hoá, bên nhận sử dụng khoá bí mật của mình để giải mã và lấy ra thông tin ban đầu.

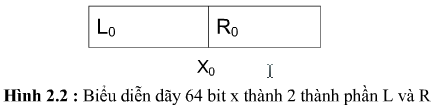
## Cơ chế mã hóa DES? Trình bày, giải thích các biện pháp nâng cao tính bảo mật DES?

Trong phương pháp DES, kích thước khối là 64 bit. DES thực hiện mã hóa dữ liệu qua 16 vòng lặp mã hóa, mỗi vòng sử dụng một khóa chu kỳ 48 bit được tạo ra từ khóa ban đầu có độ dài 56 bit.

Quá trình mã hóa của DES có thể tóm tắt như sau: Biểu diễn thông điệp nguồn x є P bằng dãy 64 bit. Khóa k có 56 bit. Thực hiện mã hóa theo 3 giai đoạn :

1. Tạo dãy 64 bit x0 bằng cách hoán vị x theo hoán vị IP (Initial Permutation)

Biểu diễn x0­= IP(x)=L0R0, L0 gồm 32 bit bên trái của x0. R0 gồm 32 bit bên phải của x0.



1. Thực hiện 16 vòng lặp từ 64 bit thu được và 56 bit của khóa k (chỉ sử dụng 48 bit của khóa k trong mỗi vòng lặp). 64 bit kết quả thu được qua mỗi vòng lặp sẽ là đầu vào cho vòng lặp sau. Các cặp từ 32 bit Ln, Rn (với 1 ≤ n ≤ 16) được xác định theo quy tắc sau:

Ln+1 = Rn

Rn+1 = Ln f (Rn, Kn+1)

Thực hiện phép XOR trên hai dãy bit, K1, K2, ...,K16 là các dãy 48 bit phát sinh từ khóa K cho trước (trên thực tế, mỗi khóa Kn được phát sinh bằng cách hoán vị các bit trong khóa K cho trước)

1. Áp dụng hoán vị ngược IP-1 đối với dãy bit R16L16, thu được từ y gồm 64 bit. Như vậy, y=IP-1 (R16L16)

Hàm f được sử dụng ở bước 2 là hàm số gồm 2 tham số: Tham số thứ nhất A là một dãy 32 bit, tham số thứ hai J là một dãy 48 bit. Kết quả của hàm f là một dãy 32 bit. Các bước xử lý của hàm f(A,J) như sau:

* Tham số thứ nhất A (32 bit) được mở rộng thành dãy 48 bit được phát sinh từ A bằng cách hoán vị theo một thứ tự nhất định 32 bit của A, trong đó có 26 bit của A được lặp lại 2 lần trong E (A).
* Thực hiện phép XOR cho 2 dãy 48 bit E(A) và J, ta thu được một dãy 48 bit B. Biểu diễn B thành từng nhóm 6 bit như sau: B= B1­ B2 B3 B4 B5 B6 B7 B8. Sử dụng 8 ma trận S­1, S2, ..., S8 mỗi ma trận Sn có kích thước 4x16 và mỗi dòng của ma trận nhận đủ 16 giá trị từ 0 đến 15. Xét dãy gồm 6 bit Bj= b1 b2 b3 b4 b5 b6, Sj(Bj) được xác định bằng giá trị của phần tử tại dòng r cột c của Sj, trong đó, chỉ số dòng r có biểu diễn nhị phân là b1 b6, chỉ số cột c có biểu diễn nhị phân là b2 b3 b4 b5­. Bằng cách này ta xác định được các dãy 4 bit Cj=Sj(Bj), 1 ≤ j ≤ 8.
* Tập hợp các dãy 4 bit Cj lại, ta có được dãy 32 bit C= C1 C2 C3 C4 C5 C6 C7 C8. Dãy 32 bit thu được bằng cách hoán vị C theo một quy luật P nhất định chính là kết quả của hàm F(A,J).
* Quá trình giải mã chính là thực hiện theo thứ tự đảo ngược tất cả các thao tác của quá trình mã hóa.

**Các biện pháp nâng cao tính bảo mật DES:**

* Triple DES (3DES): 3DES cải thiện độ mạnh của DES bằng việc sử dụng một quá trình mã hoá và giải mã sử dụng 3 khoá. Khối 64-bits của bản rõ đầu tiên sẽ được mã hoá sử dụng khoá thứ nhất. Sau đó, dữ liệu bị mã hóa được giải mã bằng việc sử dụng một khoá thứ hai. Cuối cùng, sử dụng khoá thứ ba và kết quả của quá trình mã hoá trên để mã hoá.
* AES(Advanced Encryption Standard) được sử dụng để thay thế cho DES. Nó hỗ trợ độ dài của khoá từ 128 bits cho đến 256 bits.

## Cơ chế mã hóa nào được dùng để thay thế DES? Trình bày cơ chế đó. Các ưu điểm của cơ chế đó so với DES?

Cơ chế mã hóa DES được thay thế bằng cơ chế mã hóa AES (viết tắt của từ tiếng Anh: Advanced Encryption Standard hay Tiêu chuẩn mã hóa tiên tiến).

**Cơ chế mã hóa AES** là một thuật toán mã hóa khối được chính phủ Hoa kỳ áp dụng làm tiêu chuẩn mã hóa. Giống như tiêu chuẩn tiền nhiệm DES, AES được kỳ vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kỹ lưỡng. AES được chấp thuận làm tiêu chuẩn liên bang bởi Viện tiêu chuẩn và công nghệ quốc gia Hoa kỳ (NIST) sau một quá trình tiêu chuẩn hóa kéo dài 5 năm. Thuật toán được thiết kế bởi hai nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen.

AES làm việc với các khối dữ liệu (đầu vào và đầu ra) 128 bít và khóa có độ dài 128, 192 hoặc 256. Hầu hết các phép toán trong thuật toán AES đều thực hiện trong một trường hữu hạn của các byte. Mỗi khối dữ liệu 128 bit đầu vào được chia thành 16 byte (mỗi byte 8 bit),có thể xếp thành 4 cột, mỗi cột 4 phần tử hay là một ma trận 4x4 của các byte,nó được gọi là ma trận trạng thái. Trong quá trình thực hiện thuật toán các toán tử tác động để biến đổi ma trận trạng thái này.

**\* Ưu điểm so với DES:**

+ DES (Data Encryption Standard) là kiểu mã hóa khá cũ. AES mới hơn và tốt hơn.

+ DES mã hóa có thễ phá vỡ bằng một số phương pháp tấn công. AES không thể bị phá vỡ.

+ DES sử dụng “bit encryption key” (độ dài chìa khóa mã hóa) rất ngắn 56 bit. Với 56bit có tối đa 256 kết hợp có vẻ như rất nhiều, nhưng là khá dễ dàng cho một máy tính để làm một cuộc tấn công. Còn đối với AES sử dụng 128bit, 192bit, hoặc 256bit với 2 ^ 128, 2 ^ 192, 2 ^ 256 kết hợp tương ứng. Các khóa mã hóa còn làm cho nó khó khăn hơn nhiều để phá vỡ.

+ DES có “bit blocks” (kích thước khối) nhỏ là 64 bit. Trong khi đó, AES sử dụng bit blocks gấp hai lần là 128 bit.

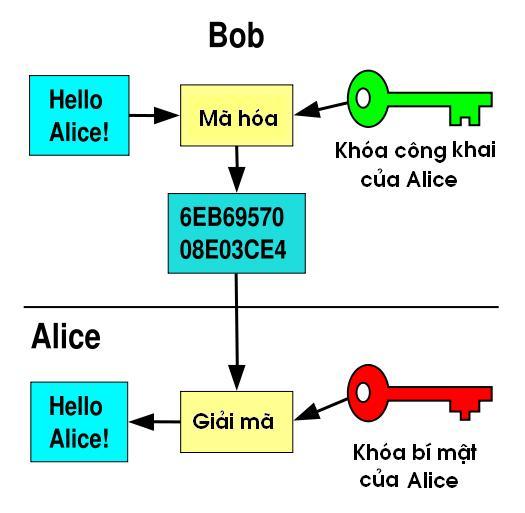
+ Xét về cơ cấu, DES sử dụng “Balanced Feistel network” chia khối thành hai nửa trước khi đi qua các bước mã hóa. Mặt khác, AES sử dụng “Substitution Permutation network” trong đó bao gồm một loạt các thay thế và hoán vị các bước để tạo ra các khối mã hóa.

## Cách thức mã hóa RSA?

**Thuật toán RSA có hai Khóa:**

+ Khóa công khai (Public key): được công bố rộng rãi cho mọi người và được dùng để mã hóa

+Khóa bí mật (Private key): Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng



**Tạo khóa**

+ Bước 1: B (người nhận) tạo hai số nguyên tố lớn ngẫu nhiên p và q

+ Bước 2: Tính n=p\*q và Φ(n) = (p-1)(q-1)

+ Bước 3: Chọn một số ngẫu nhiên e

(0< e < Φ(n)) sao cho ƯCLN(e,Φ(n))=1

+ Bước 4: Tính  bằng cách dùng thuật toán Euclide

Tìm số tự nhiên x sao cho 

+ Bước 5:

- n và e làm khoá công khai (public key),

- d làm khoá bí mật (pivate key).

**Mã hóa và giải mã**

+ Bước 1: A nhận khoá công khai của B.

+ Bước 2: A biểu diễn thông tin cần gửi thành số m (0 <= m <= n-1)

+ Bước 3: Tính c=modn

+ Bước 4: Gửi c cho B

+ Bước 5: Giải mã

tính m=modn

=> m là thông tin nhận được.

# Phần 2: Authentication

## Kĩ thuật nào giả dạng IP Source/Destination?

Man-in-the-middle

Playback

IP address spoofing

Session hijacking

IP source routing

Flying-Blind

Ping of death

SYN flood

Land Attack

Smurf attack

## Nêu đặc điểm, tính chất, cơ chế của các dạng tấn công mạng sau: spoofing, man-in-the-middle, playback, Hijacking.

**Spoofing:**

+ Trong an ninh mạng, một cuộc tấn công “spoofing” là một kiểu tấn công trong đó một người hay một chương trình giả dạng thành công như là một bằng làm sai lệch dữ liệu nhằm mục đích không chính đáng.

+ Một cuộc Spoofing attack là khi một bên nguy hiểm đóng giả một thiết bị khác hoặc người sử dụng trên một mạng để tiến hành các cuộc tấn công chống lại các máy chủ, ăn cắp dữ liệu, lay lan phần mềm độc hại hoặc truy cập trái phép. Một số trong những phương pháp phổ biến nhất bao gồm các cuộc tấn công giả IP spoofing, các cuộc tấn công ARP spoofing và tấn công spoofing DNS server.

**Man-in-the-middle**

+ Trong mật mã và an ninh máy tính, một cuộc tấn công man-in-the-middle (thường viết tắt là MITM, MITM, MIM, MIM hoặc MITMA) là một cuộc tấn công mà kẻ tấn công bí mật chuyển tiếp và có thể thay đổi các thông tin liên lạc giữa hai bên khiến họ tin rằng họ đang trực tiếp giao tiếp với nhau.

+ Giả sử Alice muốn giao tiếp với Bob.Trong khi đó, Mallory muốn để đánh chặn các cuộc trò chuyện để nghe trộm và có thể cung cấp một thông điệp sai lầm cho Bob. Đầu tiên, Alice hỏi Bob cho khóa công khai của mình. Bob sẽ gửi khóa công khai của mình cho Alice, nhưng Mallory là khả năng đánh chặn nó, một cuộc tấn công man-in-the-middle có thể bắt đầu. Mallory gửi một thông điệp giả mạo để Alice rằng đó là từ Bob, nhưng thay vì vậy đó là khóa công khai của Mallory. Alice, tin khóa công khai này là Bob, Alice mã hóa thông điệp của mình và gửi tin nhắn lại cho Bob. Mallory lại chặn, giải mã các thông điệp bằng khóa riêng của mình, có thể làm thay đổi nó nếu cô ấy muốn, và re-encrypt nó bằng cách sử dụng khóa công khai ban đầu Bob gửi cho Alice. Sau đó sẽ chuyển tiếp nó đến Bob, Bob nhận được tin nhắn mới ông tin rằng nó đến từ Alice.

**PlayBlack**

+ Một cuộc tấn công Playblack (còn được gọi là cuộc tấn công phát lại) là một hình thức tấn công mạng, trong đó một dữ liệu truyền tải bị lặp đi lặp lại hoặc trì hoãn do những kẻ cố tình ghi lại nó. Nó có thể là một phần của cuộc tấn công khác.

+ Giả sử Alice muốn chứng minh danh tính của cô với Bob. Bob yêu cầu mật khẩu của cô ấy như là bằng chứng về danh tính Alice sẵng lòng cung cấp nó (có thể sau khi mã hóa thành một hàm băm). Trong khi đó, Eve là nghe trộm cuộc nói chuyện và giữ mật khẩu (hoặc hàm băm). Sau khi trao đổi xong, Eve (giả như Alice) kết nối với Bob; khi được hỏi về xác minh danh tính, Eve sẽ gửi mật khẩu của Alice ( hoặc hàm băm) đọc từ phiên giao dịch trước, mà Bob xác nhận là của Alice do đó cấp quyền truy cập cho Eve.

**Hijacking**

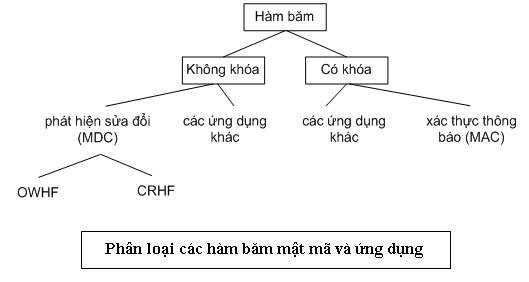
+ Hijacking là một loại tấn công an ninh mạng, trong đó kẻ tấn công chiếm quyền điều khiển của một giao tiếp – giống như là một tên không tặc làm mất kiểm soát của một chuyến bay . Man-in-the-middle cũng được biết đến như một kiểu Hijacking. Hiểu đơn giản Hijacking là “take over” tiếp tục kết nối bằng cách loại bỏ đi người gửi hoặc người nhận và thay chỗ mình vào.

# Phần 3: Integrity

## Hàm băm là gì? Có mấy loại hàm băm? Tính chất của hàm băm?

Hàm băm (Hash function)là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ ‘’lọc’’ băm thông điệp được đưa vào theo một thuật toán ***h*** một chiều nào đó, rồi đưa ra một bản băm – văn bản đại diện – có kích thước cố định. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm.

**Phân loại Hàm băm**

Có 2 loại: hàm băm không khóa và hàm băng có khóa

**Tính chất hàm băm**

Với thông điệp đầu vào *x* thu được bản băm ***z* = *h*(*x*)** là duy nhất.

Nếu dữ liệu trong thông điệp *x* thay đổi để thành thông điệp *x*’ thì ***h*(*x*’) ≠*h*(*x*)** => Hai thông điệp hoàn toàn khác nhau thì giá trị hàm băm cũng khác nhau.

Nội dung của thông điệp gốc không thể bị suy ra từ giá trị hàm băm => Với thông điệp *x* thì dễ dàng tính được *z* = *h*(*x*), nhưng lại không thể (thực chất là khó) suy ngược lại được *x* nếu chỉ biết giá trị hàm băm *h.*

## Chữ ký số là gì? Các đặc điểm của chữ ký số?

Chữ kí số là một giao thức tạo ra một hiệu quả tương tự như chữ kí thực:

Nó là một dấu hiệu mà chỉ có người gửi mới có thể tạo ra nhưng những người khác có thể nhận thấy được rằng nó là của người gửi.

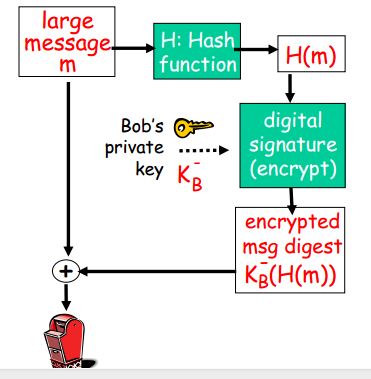
Giống như chữ kí thực, chữ kí số dùng để xác nhận nội dung thông báo.

**Đặc điểm của chữ kí số:**

* Bảo mật dữ liệu(mã hóa).
* Xác thực danh tính(chống giả mạo).
* Toàn vẹn dữ liệu(đảm bảo tính chính xác của dữ liệu, chống giả mạo).
* Chống chối bỏ trách nhiệm(bảo vệ quyền lợi cho người kí, người thi hành).

## Hãy miêu tả cách thức hoạt động của việc xác nhận tính toàn vẹn nội dung của một message?

Giả sử Bob muốn gửi tin nhắn cho Alice . Lúc này tin nhắn của Bob nội dung sẽ được mã hóa bằng hàm băm (hash fuction H(m) ) sau đó dùng khóa riêng của Bob (Bob’s private key ) gắn vào chữ kí số (mã hóa).

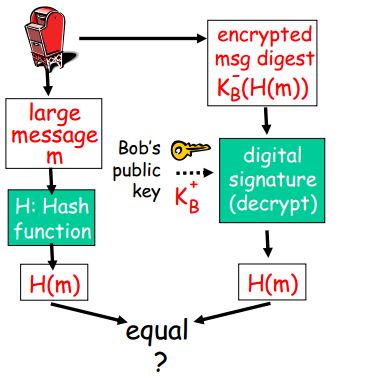


Khi tin nhắn được gửi đi sẻ chia thành hai phần nội dung và phần chữ kí đã được mã hóa.

+ Phần nội dung: sẽ dùng hàm băm mã hóa tìm giá trị H(m)

+ Phần chữ kí đã được mã hóa sẽ được gắn khóa công khai của Bob (Bob’s public key) để tiến hành giải mã tìm ra giá trị H(m).

Tiến hành so sánh hai giá trị H(m) nếu trùng khớp thì nội dung tin nhắn đã không bị thay đổi đảm bảo tính toàn vẹn (Integrity)



# Phần 4: Key Distribution & Certification

## KDC dùng để làm gì? Cơ chế hoạt động.

 KDC(Key Distribution Center) bao gồm hai chức năng: "máy chủ xác thực" (authentication server - AS) và "máy chủ cung cấp ticket" (ticket granting server - TGS). Ticket trong hệ thống Kerberos chính là các chứng thực chứng minh tính hợp lệ của người sử dụng.

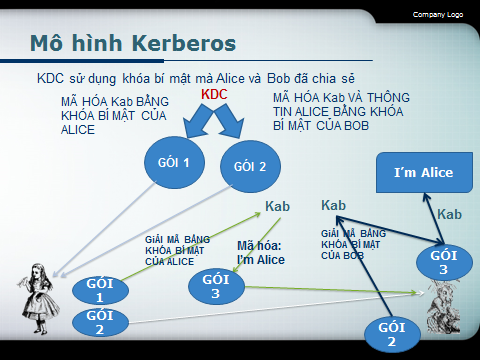
**Cơ chế hoạt động KDC**

**Tình huống:**

Alice muốn nói chuyện với Bob 🡪 Gửi yêu cầu đến KDC

KDC tạo ra một Session Key gọi tắt là Kab, sử dụng để mã hóa dữ liệu truyền giữa Alice và Bob.

**Vậy** làm sao gửi Kab đến Alice và Bob một cách an toàn?



## CA Server dùng để làm gì? Cơ chế hoạt động.

**CA Server dùng để làm gì?**

CA server chuyên cung cấp chứng thực cho người dùng

**Cơ chế hoạt động CA Server**

**A**

**PA**

**CRCA**

**CRCA**

**Encrypt**

**QCA**

**SA**

**A**

**PA SA**

Như vậy lúc này mỗi tài khoản người dùng sẽ tồn tại 2 Public Key và 1 Private Key

Có như vậy khi **B** nhận được một thông tin từ **A** nó sẽ đem thông tin **S** của nó giải mã với **P** của CA Server và thu được **CRC** nào đó

**B**

**SB**

**Decrypt**

**PCA**

**CRCB**

**PB**

**A->B**

Nó sẽ lấy tiếp giá trị CRC vừa thu được đem so sánh với CRC của chính mình nếu trung khớp thì cho qua. Ngược lại nó biết đây chính là nội dung không đáng tin cậy do bị sửa đổi từ trước.

## Nêu các tổ chức/cty cung cấp dịch vụ KDC, CA ở Việt Nam?

* Tập đoàn Bưu chính Viễn thông Việt Nam
* Công ty cổ phần Công nghệ Thẻ Nacencomm
* Công ty TNHH Hệ thống Thông tin FPT
* Tập đoàn Viễn thông Quân đội Viettel
* Công ty TNHH An ninh mạng Bkav
* Công ty Công nghệ và Truyền thông CK
* Công ty cổ phần Truyền thông Newtelecom
* Công ty cổ phần Chữ ký số Vi Na

## Tác dụng của Certification là gì? Liệt kê các trường thông tin chính trong 1 certification.

**Tác dụng của certification.**

Đảm bảo dữ liệu chuyển đi không bị đánh cắp.

Có khả năng xác thực, tránh trường hợp giả danh, mạo nhận.

Có khả năng kiểm tra tính toàn vẹn dữ liệu.

## IPSec dùng cơ chế Symmetric hay Asymmetric Key? Thuật toán mã hóa của nó là gì? Mô tả cơ chế bảo mật của IPSec.

**IPSec dùng cơ chế Symmetric hay Asymmetric Key?**

IPSec dùng cả 2 cơ chế là Symmetric và Asymmetric key.

**IPSec có 3 bộ giao thức sử dụng thuật toán mã hóa khác nhau.**

1. **Internet Key Exchange – IKE**

Trong quá trình trao đổi key IKE dùng thuật toán mã hóa đối xứng (Symmetrical Encrytion) để bảo vệ việc trao đổi key giữa các thiết bị tham gia

1. **Encapsulation Security Payload – ESP**
2. **Authentication Header – AH**

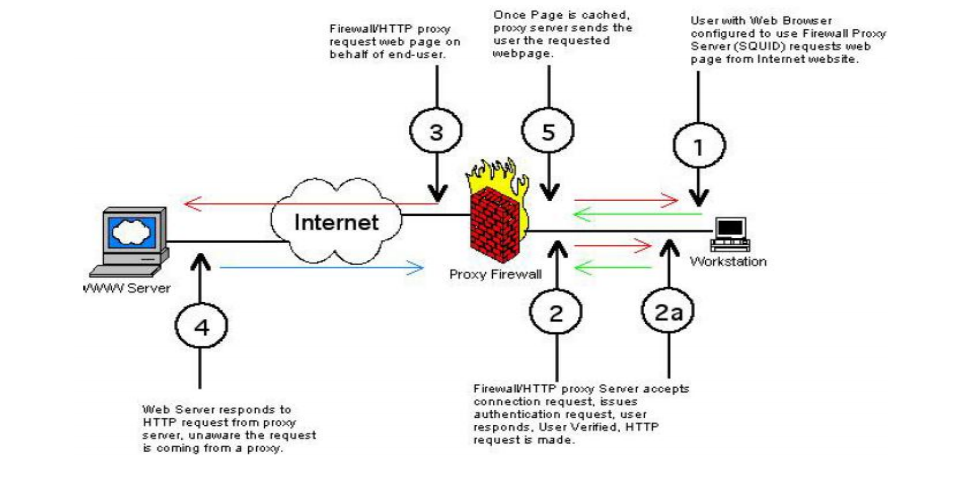
# Phần 5: Firewall

## Nhiệm vụ chung của Firewall? chức năng của Firewall trên môi trường mạng Internet?

1. **Nhiệm vụ chung của Firewall.**

* Nhiệm vụ cơ bản của tường lửa là kiểm soát đường truyền dữ liệu giữa hai vùng tin cậy khác nhau: Mạng internet (đường truyền không đáng tin cậy) và mạng nội bộ (đường truyền có độ tin cậy cao)
* Bảo vệ thông tin : bảo vệ các dữ liệu quan trọng trong hệ thống mạng nội bộ, tài nguyên hệ thống. Giúp cho doanh nghiệp, tổ chức an toàn thông tin.
* Phòng thủ các cuôc tấn công: Ngoài việc bảo vệ  các thông tin từ bên trong hệ thống ,Firewall còn có thể chống lại các cuộc tấn công từ bên ngoài  như :
  + Hacker thường sử dụng một số chương trình có khả năng dò tìm các thông tin về hệ thống nhằm phát hiện lỗi của hệ thống và dó tìm tài khoản và password của người quản trị . Firewall có khả năng phát hiện và ngăn chặn kịp thời các tấn công trên.
  + Sniff là một chương trình có khả năng bắt gói tin khi nó truyền tải trên hệ thống mạng  thì firewall có khả năng phát hiện và ngăn chặn các chương trinh đó.

1. **Chức năng của Firewall trên môi trường mạng internet.**

* Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet.
* Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet.
* Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).
* Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).
* Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.
* Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
* Kiểm soát người sử dụng và việc truy nhập của người sử dụng.
* ****Kiểm soát nội dung thông tin lưu chuyển trên mạng.

***Hình 5.1.1: một số chức năng của firewall***

## Có mấy loại Firewall theo cơ chế hoạt động? Chức năng cơ chế của mỗi loại.

1. **Có mấy loại Firewall theo cơ chế hoạt động.**

Nếu dựa vào cơ chế hoạt động thì Firewall được chia làm 2 loại chính: Application Level firewalls và IP Packet Filter Firewalls.

Ngoài ra, có thể xem: Circuite-level Gateway; Stateful Inspection Firewall; Bastion Host là một trong các loại firewall khác.

1. **Chức năng cơ chế của mỗi loại.**
2. **Firewall tầng ứng dụng (Application Level firewalls)**
   1. **Chức năng**

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng.

Bảo vệ hệ thống mạng bên trong, ngăn chặn các tấn công được khởi tạo thông qua các ứng dụng.

* 1. **Cơ chế**

Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service. Proxy service là các bộ code đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

1. **Firewall lọc gói (IP Packet Filter Firewalls)**
   1. **Chức năng.**

Firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép

* 1. **Cơ chế.**

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua Firewall thì điều đó có nghĩa rằng Firewall hoạt động chặt chẽ với giao thức TCI/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS...) thành các gói dữ liệu (data pakets) rồi gán cho các paket này những địa chỉ để có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các packet và những con số địa chỉ của chúng.

Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (packet header), dùng để cho phép truyền các packet đó ở trên mạng. Đó là:

- Địa chỉ IP nơi xuất phát ( IP Source address)

- Địa chỉ IP nơi nhận (IP Destination address)

- Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)

- Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)

- Cổng TCP/UDP nơi nhận (TCP/UDP destination port)

- Dạng thông báo ICMP (ICMP message type)

- Giao diện packet đến (incomming interface of packet)

- Giao diện packet đi (outcomming interface of packet)

Nếu luật lệ lọc packet được thoả mãn thì packet được chuyển qua firewall. Nếu không packet sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) được phép mới chạy được trên hệ thống mạng cục bộ.

## So sánh ưu và khuyết điểm của các loại Firewall?

|  |  |  |
| --- | --- | --- |
| **Phân loại**  **So sánh** | **Firewall tầng ứng dụng (Application Level firewalls)** | **Firewall lọc gói (IP Packet Filter Firewalls)** |
| **Ưu điểm** | -Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.    - Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.  -Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.  -Luật lệ lọc filltering cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet. | -Đa số các hệ thống firewall đều sử dụng bộ lọc packet. Một trong những ưu điểm của phương pháp dùng bộ lọc packet là chi phí thấp vì cơ chế lọc packet đã được bao gồm trong mỗi phần mềm router.  - Ngoài ra, bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng, vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả. |
| **Khuyết điểm** | Yêu cầu các user thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Chẳng hạn, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước để nối với máy chủ chứ không phải là một bước thôi. Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet. | -Việc định nghĩa các chế độ lọc package là một việc khá phức tạp; đòi hỏi người quản trị mạng cần có hiểu biết chi tiết vể các dịch vụ Internet, các dạng packet header, và các giá trị cụ thể có thể nhận trên mỗi trường. Khi đòi hỏi vể sự lọc càng lớn, các luật lệ vể lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển.  - Do làm việc dựa trên header của các packet, rõ ràng là bộ lọc packet không kiểm soát được nôi dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu. |

# Phần 6: Attacks and Counter measures

## Tấn công dạng Mapping được dùng để làm gì? Cơ chế tấn công. Cách phòng chống.

**Mục đích:**

Tấn công dạng Mapping dùng để lập sơ đồ mạng, nhận dạng mô hình mạng và bao nhiêu nút mạng dựa vào địa chỉ IP và vị trí của chúng trong mạng. Xác định những dịch vụ mạng đang được triển khai.

**Cơ chế:**

1. **Lập sơ đồ mạng (Network Mapping)**

Có một số công cụ bảo mật mạng chuyên nghiệp để quản lý mạng. Một vài công cụ miễn phí trong khi một số khác phải trả phí. Các công cụ mà nhiều Hacker sử dụng là Traceroute, Nmap.v.v.v.

* Traceroute là công cụ dòng lệnh nền tảng Windows dùng để xác định đường đi từ nguồn tới đích. Traceroute tìm đường tới đích bằng cách gửi các thông báo Echo Request ICMP tới từng đích. Sau mỗi lần gặp một đích, giá trị Time to Live (TTL) sẽ được tăng lên cho tới khi gặp đúng đích cần đến. Đường đi được xác định từ quá trình này.
* Nmap là một công cụ mã nguồn mở cho phép thăm dò mạng và kiểm toán an ninh. Nó được thiết kế để nhanh chóng quét các mạng lớn, xác định các chương trình đang hoạt động, các dịch vụ, các loại bộ lọc, tường lửa và các ứng dụng của hệ điều hành. Đây là một chương trình kiếm soát hệ thống mạng rất hữu ích.

1. **Quét mạng (Sweeping the Network)**

Khi sơ đồ mạng cơ bản được hoàn thành, Hacker cần tìm hiểu chi tiết hơn các nút trong mạng đích:

* Xác định hệ thống có đang "sống" hay không.
* Kiểm tra các port nào đang mở.
* Xác định những dịch vụ nào đang chạy tương ứng với các port đang mở.
* Xác định hệ điều hành và phiên bản của nó.
* Kiểm tra lỗi của những dịch vụ đang chạy.
* Xây dựng sơ đồ những host bị lỗi.

Xác định những host trong hệ thống đang sống hay chết rất quan trọng vì có thể Hacker ngừng tấn công khi xác định hệ thống đã chết. Việc xác định hệ thống có sống hay không có thể sử dụng kỹ thuật Ping Sweep.

Bản chất của quá trình này là gửi hàng loạt ICMP Echo Request đến 1 dải địa chỉ host mà hacker đang muốn tấn công và chờ  ICMP Reply. Dựa vào danh sách những host đáp ứng có thể xác định dải địa chỉ IP đang được dùng trong mạng

Từ sơ đồ chi tiết về mạng, hacker có thể tấn công dựa trên các lỗ hổng của ứng dụng, hệ điều hành .v.v.v

**Cách phòng chống**

\_ Lưu lại traffic vào mạng.

\_ Cài đặt firewall, IPS …

\_ Theo dõi các hoạt động đáng ngờ (IP, ports được quét theo chu kỳ).

\_ Tắt các ports không cần thiết.

## Packet sniffing được dùng để làm gì? Cơ chế tấn công. Cách phòng chống.

**Mục đích:**

Packet sniffing là phương pháp nghe lén dữ liệu trong quá trình truyền dữ liệu giữa các mạng.

\_ Hacker dùng nó để khai thác dữ liệu nhạy cảm: tài khoản, mật khẩu, email không được mã hóa.

\_ Quản trị mạng dùng để theo dõi hoạt động của mạng

\_ Giúp người phát triển phần mềm gỡ lỗi

**Cơ chế:**

Công nghệ Ethernet được xây dựng trên nguyên lý chia sẻ. Theo một khái niệm này thì tất cả các máy tính trên một hệ thống mạng cục bộ đều có thể chia sẻ đường truyền của hệ thống mạng đó. Hiểu một cách khác tất cả các máy tính đó đều có khả năng nhìn thấy lưu lượng dữ liệu được truyền trên đường truyền chung đó. Như vậy phần cứng Ethernet được xây dựng với tính năng lọc và bỏ qua tất cả những dữ liệu không thuộc đường truyền chung với nó.  
  
Nó thực hiện được điều này trên nguyên lý bỏ qua tất cả những Frame có địa chỉ MAC không hợp lệ đối với nó. Khi cài Sniffer trên máy nó sẽ bật tính năng promiscuous mode trên card mạng. Từ đó có thể nhìn thấy tất cả lưu lượng thông tin từ máy A đến máy C, hay bất cứ lưu lượng thông tin giữa bất kỳ máy nào trên hệ thống mạng. Miễn là chúng cùng nằm trên một hệ thống mạng.

**Phân loại**

**a. Active**

Là Sniffing qua Switch, nó rất khó thực hiện và dễ bị phát hiện. Attacker thực hiện loại tấn công này như sau:

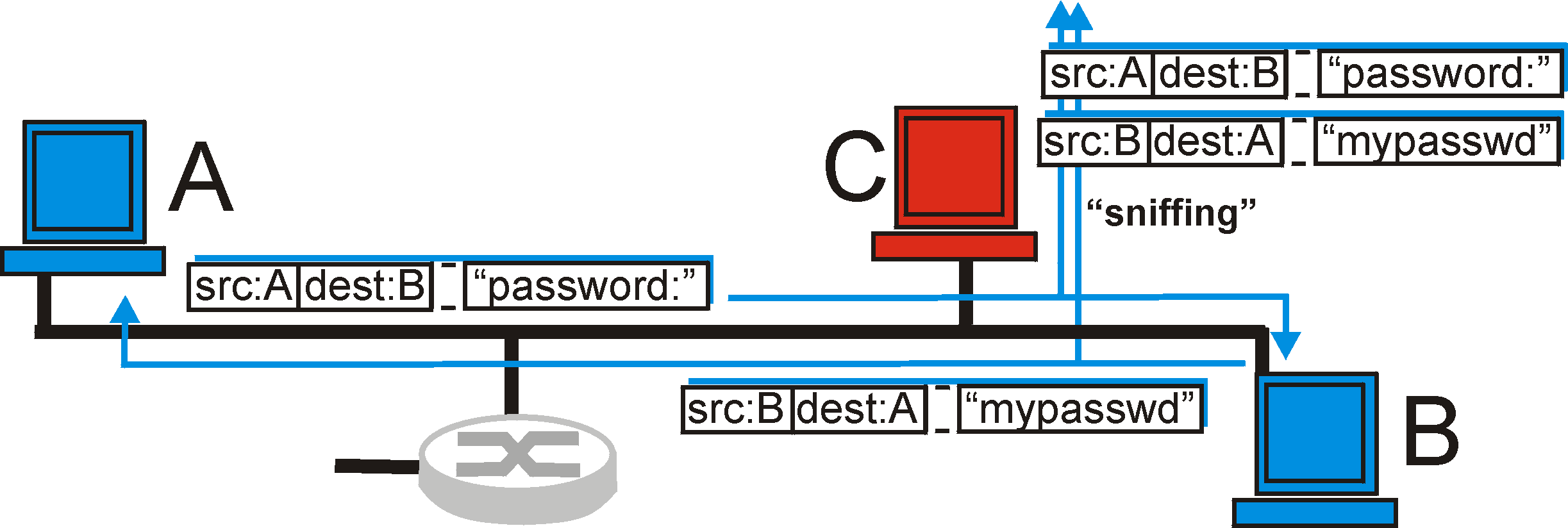
o Attacker kết nối đến Switch bằng cách gởi địa chỉ MAC nặc danh

o Switch xem địa chỉ kết hợp với mỗi khung (frame)

o Máy tính trong LAN gởi dữ liệu đến cổng kết nối

**b. Passive**

Đây là loại Sniffing lấy dữ liệu chủ yếu qua Hub. Nó được gọi là Sniffing thụ động vì rất khó có thể phát hiện ra loại Sniffing này. Attacker sử dụng máy tính của mình kết nối đến Hub và bắt đầu Sniffing



Ảnh minh họa: Máy C nghe lén dữ liệu truyền giữa A và B

**Cách phòng chống**

* + - 1. **Mã hóa đường truyền**
* SSL (Secure Socket Layer)
* PGP và S/MIME
* OpenSSH
* VPNs (Virtual Private Network)
  + - 1. **Dùng Arp**

Khi gửi một Packet ARP đến một địa chỉ nào đó trong mạng (không phải Broadcast). Nếu máy tính đó trả lời lại Packet ARP bằng địa chỉ của chính nó. Thì máy tính đó đang cài đặt Sniffer ở chế độ hỗn tạp(Promiscuous Mode).

* + - 1. **Dùng DNS**

Khi bạn phát hiện được những hành động Ping liên tục với mục đích thăm dò đến những địa chỉ IP không tồn tại trên hệ thống mạng. Tiếp đó là những hành động cố gắng phân giải ngược những địa chỉ IP được biết từ những Packet ARP. Đây là những hành động của một chương trình Sniffer.

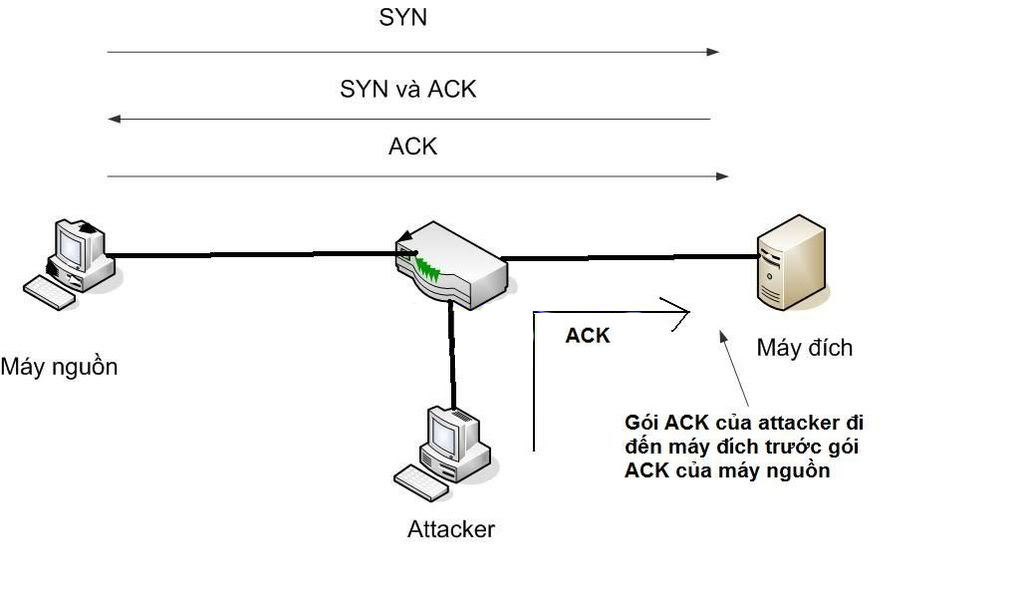
1. **Sử dụng các phương thức chứng thực mạnh như OPT.**

## Ip Spoofing được dùng để làm gì? Cơ chế tấn công. Cách phòng chống.

IP spoofing là sự giả mạo địa chỉ IP hoặc khống chế tập tin lưu trữ thông tin về địa chỉ IP của các thiết bị trong hệ thống mạng. Đây là một trong những cách thông dụng mà hacker thường dùng để mạo danh là một máy tính hợp pháp để xâm nhập một hệ thống mạng, chiếm quyền điều khiển trình duyệt web trên máy tính bị tấn công, biến máy tính đó thành một công cụ khai thác thông tin. Phương thức hoạt động là hacker truyền những gói dữ liệu do họ tạo ra với một địa chỉ IP hợp pháp của một máy tính trong mạng.

**Cơ chế**

Chúng ta đã biết trong phần đầu của những gói dữ liệu luôn có địa chỉ IP của nguồn xuất phát dữ liệu và chỉ số thứ tự (**sequence number-dùng để sắp xếp các gói dữ liệu nhận đc theo một thứ tự định sẵn**). Để có thể lấy quyền điều khiển một phiên làm việc đang thiết lâp giữa nguồn hợp pháp và một host đích,kẻ tấn công cần biết về số thứ tự đó.Nếu kẻ tấn công dự đoán đúng số thứ tự,hắn có thể gửi tới host đích một ACK segment chính xác.Khi đó ,chỉ cần ACK segment của attacker tới dc đích trước AKC segement gốc,thì attacker sẽ dc tin cậy bởi host đích ,như trong hình dưới :



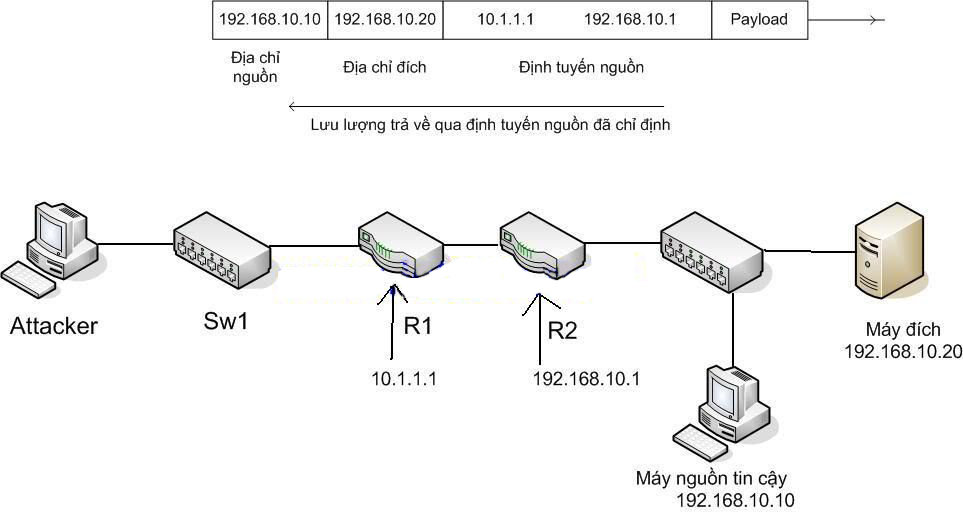
Làm thế nào attacker có thể biết chính xác số TCP sequence dựa trên cách giả mạo địa chỉ IP dc sử dụng? Ta có 2 loại giả mạo địa chỉ IP,với mỗi loại như vậy thì attacker có kỹ thuật tấn công khác nhau:

**Non-blind spoofing**:diễn ra khi máy tấn công và mục tiêu ở trên cùng một subnet.Khi đó ,attacker có thể sử dụng công cụ bắt gói ,phân tích gói tin để có thể có dc số thứ tự.

**Blind spoofing**:diễn ra khi máy tấn công khác subnet với mục tiêu.Khi đó,việc có dc số TCP sequence chính xác là rất khó.Tuy nhiên ,với một số kĩ thuật,chẳng hạn như **IP source routing**,máy tấn công cũng có thể xác định chính xác dc chỉ số đó.

**IP source routing**

**IP source routing** là một cơ chế cho phép một máy nguồn chỉ ra đường đi một cách cụ thể và không phụ thuộc vào bảng định tuyến của các router.  
  
Nếu attacker dũng kỹ thuật **IP source routing** ,hắn có thể nhắm tới một đường định tuyến thành công đã có sẵn.Máy tấn công lúc này có thể gởi một gói IP với địa chỉ nguồn tự tạo trong IP header.Và khi host đích nhận dc gói tin này,nó sẽ gửi traffic ngược lại đến địa chỉ IP giả mạo thông qua đường router mà attacker muốn.Cách tiếp cận này có thể vượt qua những khó khăn khi thực hiện việc tấn công **blind spoofing.**

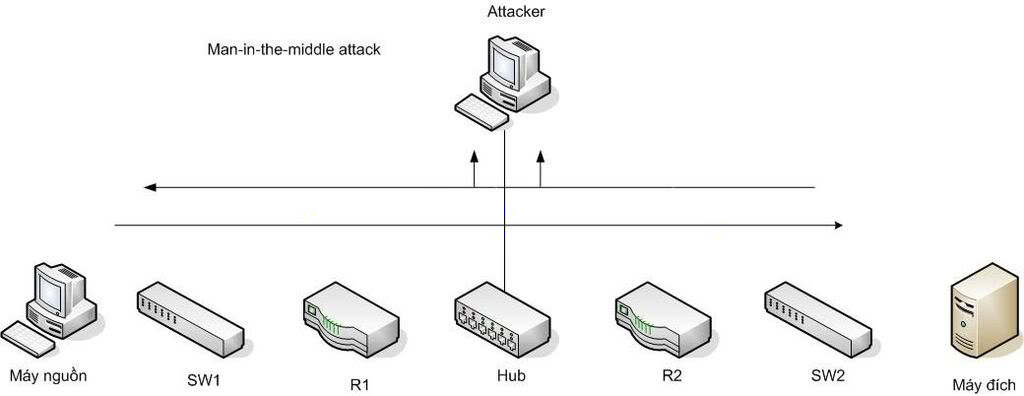


**MAN-IN-THE-MIDDLE**

Nếu một máy tấn công có cùng subnet với máy nạn nhân,hắn có thể sử dụng cách tấn công này.Một trong những cách tấn công người ở giữa (man-in-the-middle) là kẻ tấn công làm cách nào đó để hệ thống gởi frame qua PC của mình.Chẳng hạn,attacker có thể gửi hàng loạt những gói ARP vu vơ tới hệ thống.Những frame ARP đó có thể thông báo rằng địa chỉ MAC của attacker là địa chỉ MAC của router kế tiếp (next-hop).Do đó attacker sẽ nhận dc traffic,rồi sau đó chuyển traffic đến router kế tiếp thật sự.Và kết quả ,người dùng đầu cuối không hề biết traffic của mình đều đi qua một PC khác.

Một dạng khác của việc tấn công man-in-the-middle là khi attacker nối thiết bị hub đến một vùng mạng có mạng traffic mà attacker muốn bắt lấy,như trong hình dưới.Cách khác là attacker có thể kết nối tới một Switch Port Analyzer(SPAN) port trên Catalyst switch .Switch này seo chép traffic và chuyển chúng đến port đã cấu hình tính năng SPAN.Tính năng SPAN của switch là tính năng trong đó qui định tất cả các lưu lượng vào ra một cổng trên switch sẽ dc chép một phiên bản gửi về máy đích.

Kẻ tấn công có thể sử dụng một công cụ bắt gói và phân tích để bắt lưu lượng đang di chuyển giữa hệ thống đầu và cuối.Nếu traffic bắt dc là dạng plain text,attacker hoàn toàn có thể thu dc những thông tin nhạy cảm,chẳng hạn như thông tin người dùng và mật khẩu.



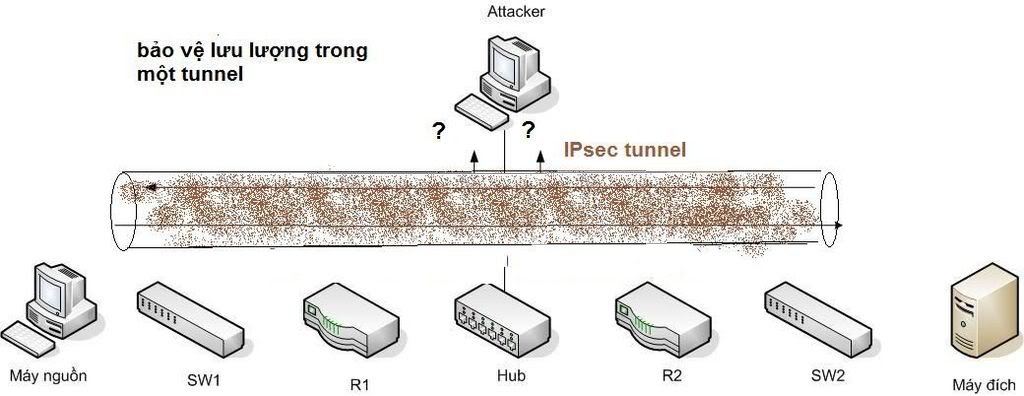
**Cách phòng chống**

Để làm giảm nguy cơ tấn công giả mạo địa chỉ IP cho một hệ thống mạng,ta có thể sử dụng các phương pháp sau:

-Dùng danh sách kiểm tra truy cập (Access Control List-ACL) trên các tinterface của router.Một ACL có thể dc dùng để loại bỏ những traffic từ bên ngoài mà lại dc đóng gói bởi một địa chỉ trong mạng cục bộ khi bị lôi cuốn vào một cuộc tấn công Ddos.Vì thế một ACL có thể loại bỏ các traffic rời khỏi mạng cục bõ có địa chỉ nguồn khác với không gian địa chỉ IP bên trong mạng nội bộ.

-Dùng mật mã xác thực.Nếu cả hai đầu của cuộc nói chuyện đã dc xác thực,khả năng tấn công theo kiểu man-in-the-middle có thể dc ngăn cản.

-Mã hoá traffic giữa các thiết bị (giữa 2 router,hoặc giữa 2 hệ thống cuối và router) bằng mộtIPSec tunnel .Trong hình dưới chú ý rằng mô hình đang dc bảo vệ bởi một IPsec tunnel.Cho dù attacker vẫn chụp dc các gói tin ,thì các gói bắt dc không thể đọc được,vì traffic đã dc mã hoa bên trong IPsec tunnel



## **Liệt kê một số giao thức, thuật toán nổi bật về Security ở từng OSI Layer**.

**Các giao thức bảo mật ở một số Layer**

**Application layer: Secure email (PGP)**

Secure email dùng:

* Symmetric Algorithm dùng mã hóa nội dung tin nhắn lúc truyền đi.
* Public key dùng để decrypt tin nhắn
* Hash function
* Digital signature tạo bằng RSA hoặc DSA thông qua hàm hash tạo từ nội dung tin nhắn bán đầu.

**Transport layer: SSL**

*Thuật toán sử dụng*: Asymmetric encryption, Symmetric encryption

Phát triển bởi Netscape với mục đích chuyển dữ liệu an toàn qua Internet.  
Sử dụng public/private key để mã hóa dữ liệu.

URLs ―https:‖ thay vì ―http:

**Network layer: Ipsec**

IPSec là một phương pháp để bảo vệ gói tin IP: Là một tiêu chuẩn của IETF

*Các thuật toán*:

HMAC-SHA1,TripleDES-CBC, AES-CBC, AES-GCM

**Link layer:** 802.11x, Point-to-Point Protocol (PPP), Point-to-Point Tunneling Protocol (PPTP)