

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ  
THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập – tự do – hạnh phúc

BỘ MÔN AN TOÀN HTTT

**GIÁO TRÌNH**  
**AN TOÀN VÀ AN NINH MẠNG**

Biên soạn: Ths. NGUYỄN VĂN LINH

Hệ đào tạo: Đại học chính quy

Lưu hành nội bộ

Thái Nguyên , 7/2016

## Mục lục

Chương 1 : TỔNG QUAN VỀ AN TOÀN THÔNG TIN .....	4
1.1 Khái niệm an toàn mạng .....	4
1.2 Các yếu tố xác lập an toàn thông tin .....	4
1.2.1 Các dịch vụ an toàn .....	4
1.2.2 Các cơ chế an toàn .....	5
1.2.3 Các hình thức tấn công .....	5
1.3 Mô hình an toàn mạng .....	8
Chương 2: MỘT SỐ PHƯƠNG PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN .....	11
2.1 Mã hóa dữ liệu .....	11
2.1.1 Cơ chế áp dụng mã hóa thông tin trên đường truyền .....	11
2.2 Lỗ hổng bảo mật và phương pháp phát hiện .....	16
2.3 Bảo mật đường truyền tải .....	21
2.4 Bảo mật mạng không dây .....	22
2.4.1 WAP .....	22
2.4.2 WEP .....	24
2.4.3 WPA,WPA2 .....	24
2.5 Bảo mật thư điện tử .....	26
2.6 An ninh mạng .....	26
2.6.1 Chính sách an ninh mạng .....	26
2.7 Vấn đề an ninh hệ thống .....	30
2.7.1 Các cơ chế đảm bảo an toàn hệ thống .....	32
2.7.3 Đảm bảo tính riêng tư cho luồng truyền tải .....	34
2.8 Trao đổi khóa và ứng dụng an toàn trên Internet .....	34
Chương 3: GIAO THÚC VÀ ỨNG DỤNG AN TOÀN .....	36
3.1 SSL .....	36
3.2 TLS .....	40
3.3 HTTPS .....	41
3.4 SSH .....	44
3.5 IPSec .....	47
3.6 S/MIME .....	52
3.7 PGP .....	53
Chương 4: AN NINH HỆ THỐNG .....	57
4.1 Kỹ thuật phát hiện xâm nhập trái phép .....	57
4.1.1. Thành phần .....	57
4.1.2 Phân loại .....	60
4.1.3 Nguyên lý hoạt động .....	64
4.1.4 Hệ thống IDS dựa trên phát hiện bất thường .....	67
	97
4.2 Phần mềm độc hại .....	97
4.2.1 Virus .....	97
4.2.2 Anti-Virus .....	101
4.3 Tường lửa .....	114

Chương 5: QUY TRÌNH THIẾT LẬP HỆ THỐNG AN NINH AN TOÀN .....	118
5.1 Phân tích, xác định các mối đe dọa .....	118
5.2 Áp dụng cơ chế phòng thủ đa lớp.....	119
5.3 Mô hình phòng thủ thế hệ mới .....	121
5.4 Đào tạo con người .....	127

CONFIDENTIAL

# Chương 1 : TỔNG QUAN VỀ AN TOÀN THÔNG TIN

## 1.1 Khái niệm an toàn mạng

An toàn và an ninh mạng xuất phát đều từ cùng một từ tiếng Anh là Security nhưng bản chất nghĩa có đôi chút khác nhau

### An toàn là gì

Nghĩa là bảo đảm sự hoạt động liên tục theo đúng thiết kế của dịch vụ cung cấp thông tin mà không bị ảnh hưởng bởi các yếu tố khác nhau.

### An ninh là gì

An ninh là đảm bảo chỉ có những người có thẩm quyền mới được truy suất, sử dụng tài nguyên thông tin.

### An ninh mạng là gì

An ninh mạng là những giải pháp và chính sách được quản trị viên áp dụng lên một mạng để giám sát và ngăn chặn các hành vi truy cập bất hợp pháp, các hành vi tấn công, chỉnh sửa hoặc hành vi làm gián đoạn dịch vụ cung cấp.

## 1.2 Các yếu tố xác lập an toàn thông tin

### 1.2.1 Các dịch vụ an toàn

Các dịch vụ an toàn an ninh của hệ thống thông tin phải đảm bảo các yêu cầu sau:

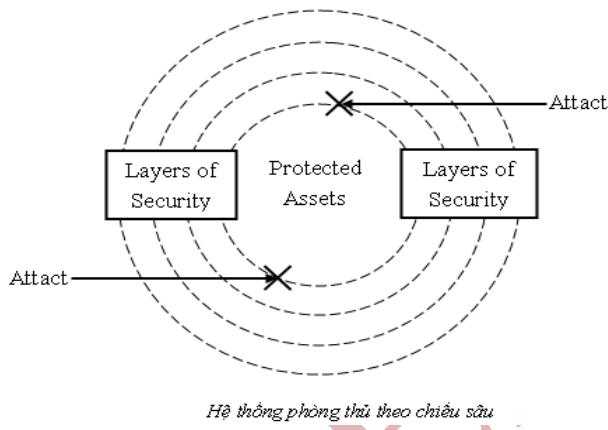
- ✓ Đảm bảo tính tin cậy: Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền.
- ✓ Đảm bảo tính nguyên vẹn: Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền.
- ✓ Đảm bảo tính sẵn sàng: Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền.
- ✓ Đảm bảo tính không thể từ chối: Thông tin được cam kết về mặt pháp luật của người cung cấp.
- ✓ Đảm bảo tính riêng tư: Bảo vệ dữ liệu được truyền tải khỏi các tấn công thụ động.
- ✓ Kiểm soát truy cập: Cung cấp khả năng giới hạn và kiểm soát các truy cập tới các máy chủ hoặc tới các ứng dụng thông qua đường truyền tin.

## 1.2.2 Các cơ chế an toàn

Trên thực tế không tồn tại một cơ chế duy nhất nào có thể đảm bảo an toàn thông tin cho mọi hệ thống.

Để đảm bảo an toàn an ninh cho hệ thống thông tin người ta sử dụng các kỹ thuật mã hóa: Mã đối xứng, mã công khai

Sử dụng Firewall, hệ thống phát hiện xâm nhập - IDS, và các biện pháp phối hợp khác.



## 1.2.3 Các hình thức tấn công

### Các hành vi dò quét:

Bất cứ sự xâm nhập vào một môi trường mạng nào đều bắt đầu bằng cách thăm dò để tập hợp thông tin người dùng, cấu trúc hệ thống bên trong và điểm yếu bảo mật. Việc thăm dò được thăm dò theo các bước thăm dò thụ động (thu thập các thông tin được công khai) và thăm dò chủ động (sử dụng các công cụ để tìm kiếm thông tin trên máy tính của nạn nhân). Các công cụ dò quét được hacker chuyên nghiệp thiết kế và công bố rộng rãi trên Internet. Các công cụ thường hay dùng: Nmap, Essential Network tools... thực hiện các hành động Ping Sweep, Packet Sniffer, DNS Zone Transfer...

### Tấn công từ chối dịch vụ( Denial Service Attacks):

Đây là kiểu tấn công khó phòng chống nhất và trên thế giới vẫn chưa có cách phòng chống triệt để. Nguyên tắc chung của cách tấn công này là hacker sẽ gửi liên tục nhiều yêu cầu phục vụ đến máy nạn nhân. Máy bị tấn công sẽ phải trả lời tất cả các yêu cầu này. Khi yêu cầu gửi đến quá nhiều, máy bị tấn công sẽ không phục vụ kịp thời dẫn đến việc đáp ứng

các yêu cầu của các máy hợp lệ sẽ bị chậm trễ, thậm chí ngừng hẳn hoặc có thể cho phép hacker nắm quyền điều khiển.

### **Các hành vi khai thác lỗ hổng bảo mật:**

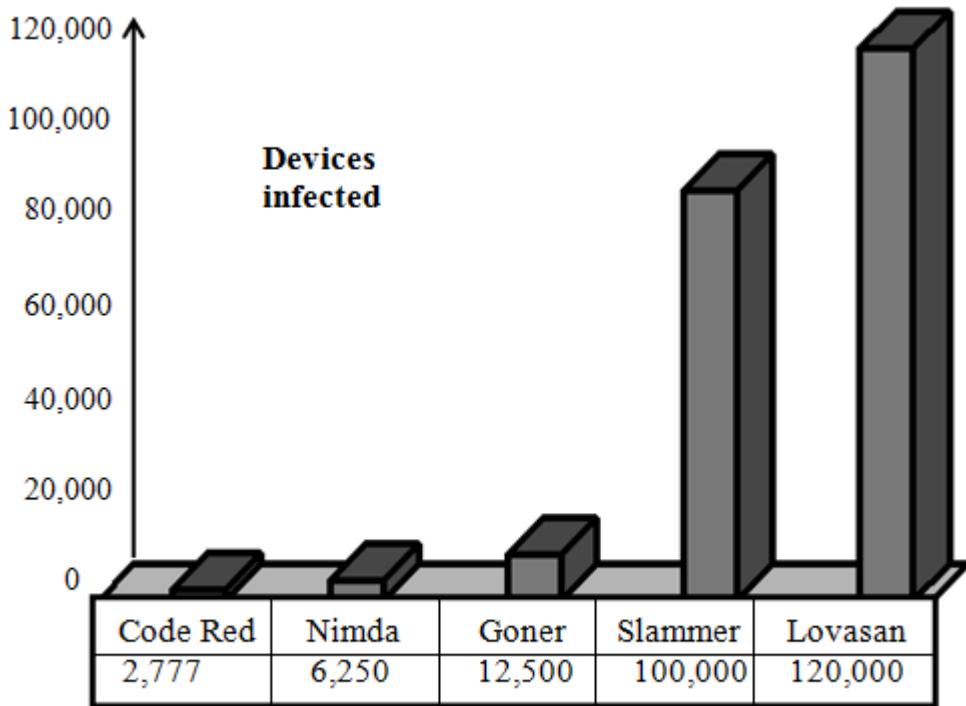
Các hệ điều hành, cơ sở dữ liệu, các ứng dụng luôn luôn có những điểm yếu xuất hiện hàng tuần thậm chí hàng ngày. Những điểm yếu này thường xuyên được công bố rộng rãi trên nhiều website về bảo mật. Do vậy các yếu điểm của hệ thống là nguyên nhân chính của các tấn công, một thống kê cho thấy hơn 90% các tấn công đều dựa trên các lỗ hổng bảo mật đã được công bố.

Đối với một hệ thống mạng có nhiều máy chủ máy trạm, việc cập nhật các bản vá lỗ hổng bảo mật là một công việc đòi hỏi tốn nhiều thời gian và khó có thể làm triệt để. Và do đó, việc tồn tại các lỗ hổng bảo mật tại một số điểm trên mạng là một điều chắc chắn. Người ta định nghĩa Tấn công Zero-Day là các cuộc tấn công diễn ra ngay khi lỗi được công bố và chưa xuất hiện bản vá lỗi. Như vậy kiểu tấn công này rất nguy hiểm vì các hệ thống bảo mật thông thường không thể phát hiện ra.

### **Các tấn công vào ứng dụng(Application-Level Attacks):**

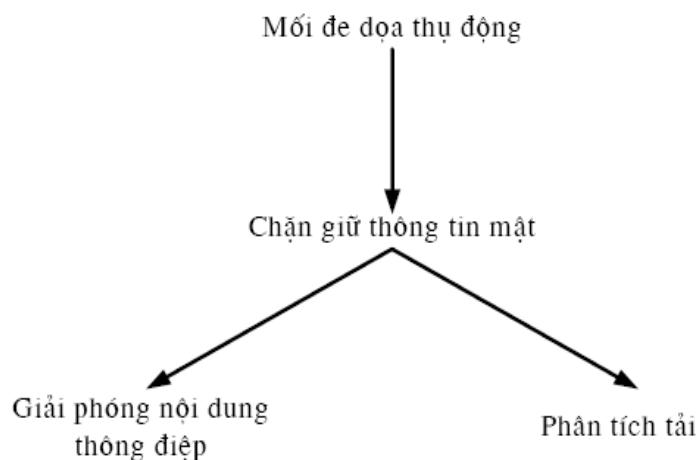
Đây là các tấn công nhằm vào các phần mềm ứng dụng mức dịch vụ. Thông thường các tấn công này, nếu thành công, sẽ cho phép kẻ xâm nhập nắm được quyền điều khiển các dịch vụ và thậm chí cả quyền điều khiển máy chủ bị tấn công.

Số lượng các vụ tấn công liên tục tăng trong khi hình thức tấn công theo kiểu dựa trên điểm yếu của con người (tấn công kiểu Sophistication) lại giảm. Rõ ràng các hình thức tấn công vào hệ thống máy tính hiện nay ngày càng đa dạng và phức tạp với trình độ kỹ thuật rất cao. Ngoài ra quá trình tấn công ngày càng được tự động hóa với những công cụ nhỏ được phát tán khắp nơi trên mạng



Số lượng máy bị tấn công ngày càng tăng (Nguồn: IDC2002)

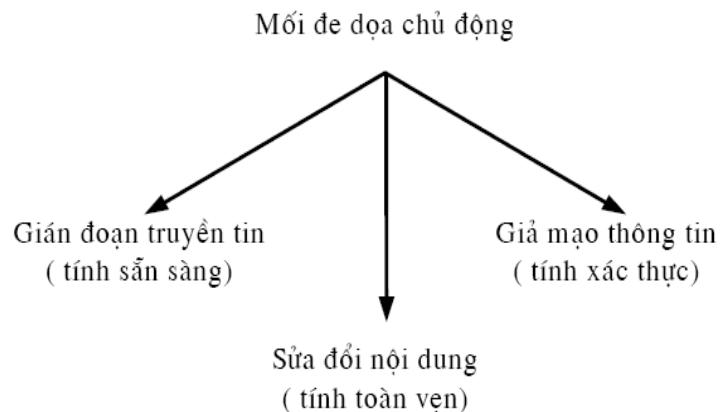
Các dạng tấn công thụ động:



- ✓ Giải phóng nội dung của thông điệp: ngăn chặn đối phương thu và tìm hiểu nội dung của thông tin truyền tải.
- ✓ Phân tích tải: Khi phân tích tải đối phương có thể xác định được vị trí của các máy tham gia vào quá trình truyền tin; tần suất và kích thước bản tin.

Dạng tấn công thụ động rất khó phát hiện vì không làm thay đổi dữ liệu, với dạng tấn công này người ta quan tâm đến vấn đề ngăn chặn hơn là vấn đề phát hiện.

### Các dạng tấn công chủ động:



- ✓ Giả danh
- ✓ Phát lại
- ✓ Thay đổi nội dung thông điệp
- ✓ Từ chối dịch vụ

Dạng tấn công chủ động rất khó có thể ngăn chặn tuyệt đối. Vì vậy yêu cầu phải bảo vệ vật lý mọi đường truyền thông tại mọi thời điểm. Mục tiêu an toàn của dạng tấn công này là có thể phát hiện và phục hồi lại thông tin từ mọi trường hợp bị phá hủy và làm trễ.

### 1.3 Mô hình an toàn mạng

Mô hình an toàn mạng: Bài toán an toàn an ninh thông tin mạng này sinh khi:

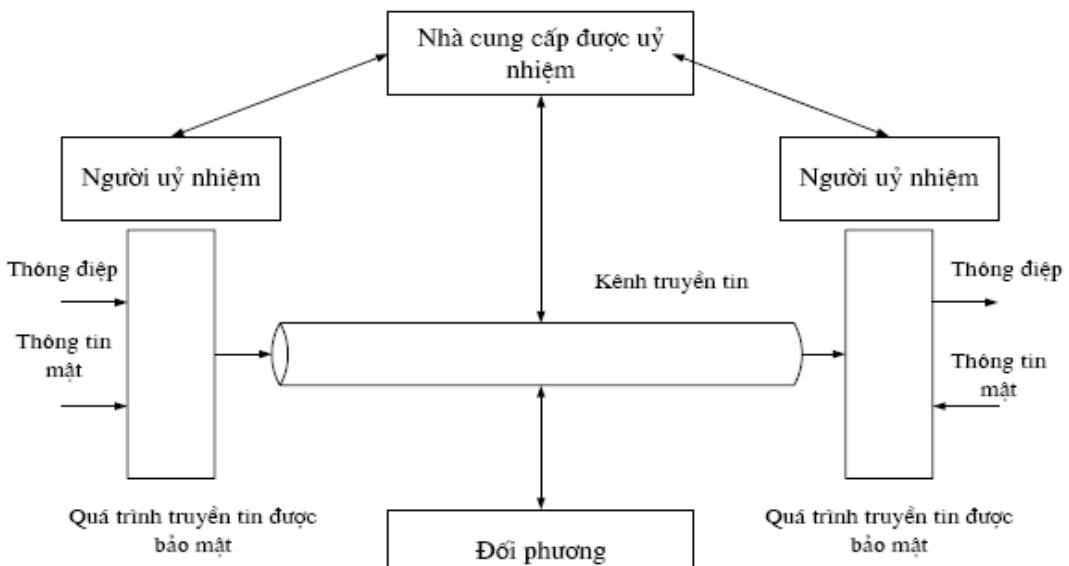
Cần thiết phải bảo vệ quá trình truyền tin khỏi các hành động truy cập trái phép

- ✓ Đảm bảo tính riêng tư và tính toàn vẹn
- ✓ Đảm bảo tính xác thực, . . .

Mô hình an toàn mạng yêu cầu:

- ✓ Thiết kế một giải thuật thích hợp cho việc chuyển đổi liên quan đến an toàn
- ✓ Tạo ra thông tin bí mật (khóa) đi kèm với giải thuật
- ✓ Phát triển các phương pháp phân bổ và chia sẻ thông tin bí mật

- ✓ Đặc tả một giao thức sử dụng bởi hai bên gửi và nhận dựa trên giải thuật an toàn và thông tin bí mật, làm cơ sở cho một dịch vụ an toàn

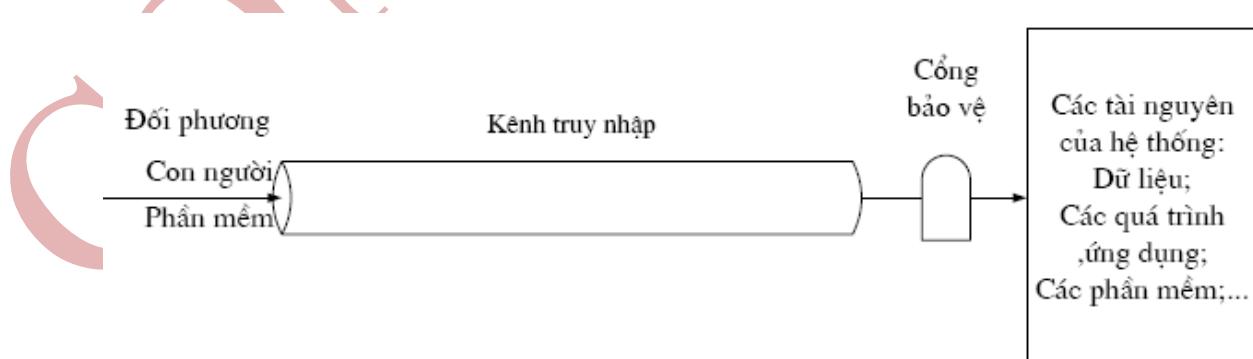


### Mô hình an toàn truy cập mạng

Mô hình này yêu cầu:

- ✓ Lựa chọn các chức năng gác cổng thích hợp để định danh người dùng
- ✓ Cài đặt các điều khiển an toàn để đảm bảo chỉ những người dùng được phép mới có thể truy nhập được vào các thông tin và tài nguyên tương ứng.

Các hệ thống máy tính đáng tin cậy có thể dùng để cài đặt mô hình này



Cần nhấn mạnh một thực tế rằng không có một hệ thống nào an toàn tuyệt đối cả. Bởi vì bất kỳ một hệ thống bảo vệ nào dù hiện đại và chắc chắn đến đâu đi nữa thì cũng có lúc bị vô hiệu hóa bởi những kẻ phá hoại có trình độ cao và có đủ thời gian. Chưa kể rằng tính an toàn của một hệ thống thông tin còn phụ thuộc rất nhiều vào việc sử dụng của con người. Từ đó có thể thấy rằng vấn đề an toàn mạng thực tế là cuộc chạy tiếp sức không ngừng và không ai dám khẳng định là có đích cuối cùng hay không.

CONFIDENTIAL

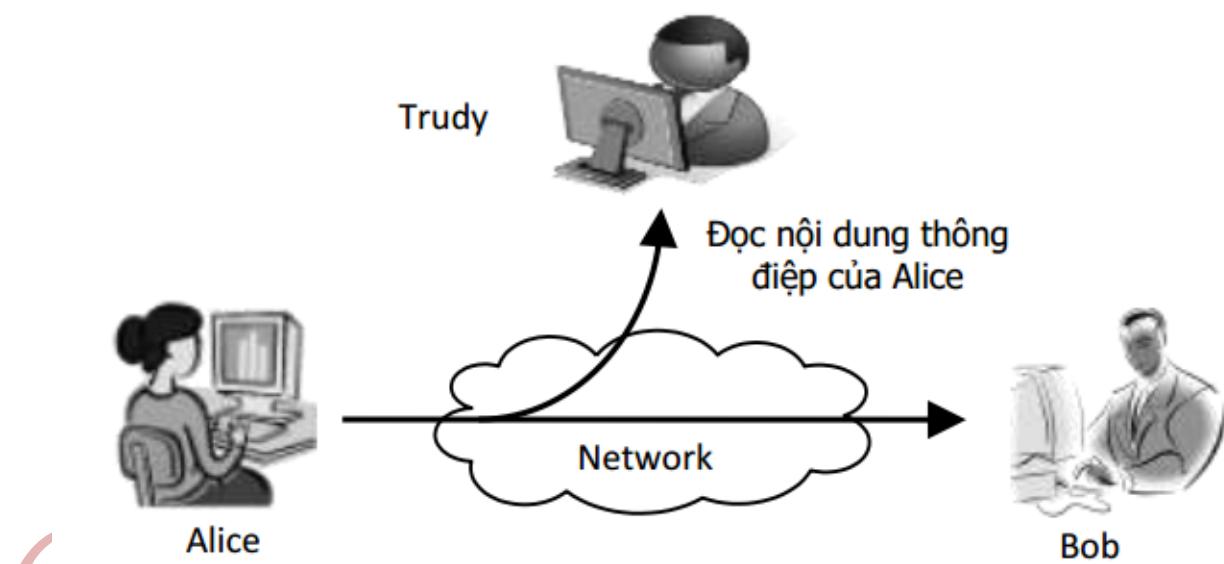
## Chương 2: MỘT SỐ PHƯƠNG PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN

### 2.1 Mã hóa dữ liệu

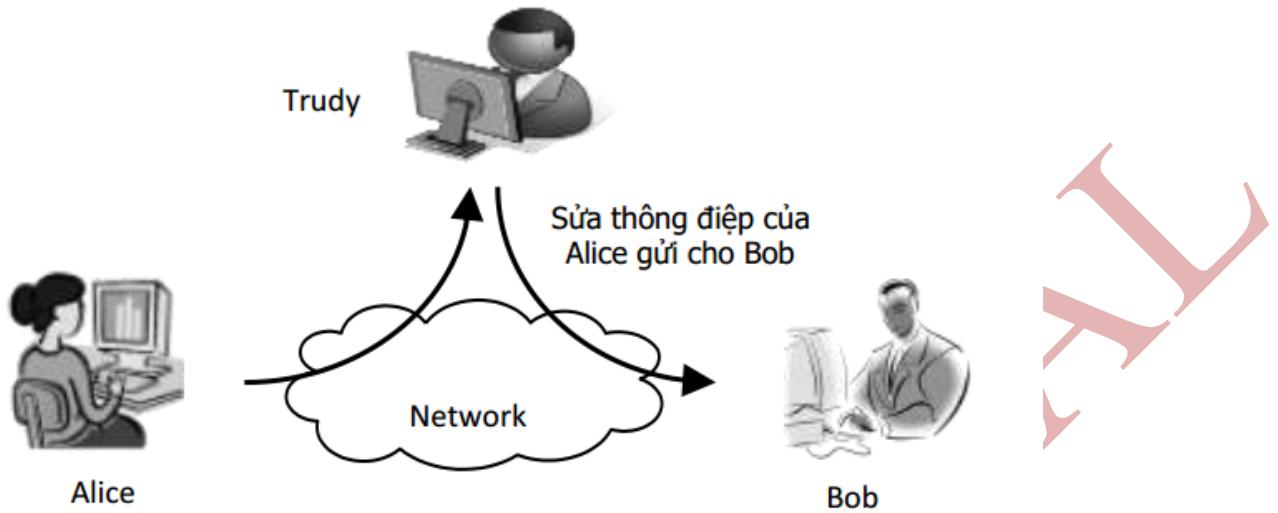
#### 2.1.1 Cơ chế áp dụng mã hóa thông tin trên đường truyền

Để xem xét những vấn đề bảo mật liên quan đến truyền thông trên mạng, chúng ta hãy lấy một bối cảnh sau: có ba nhân vật tên là Alice, Bob và Trudy, trong đó Alice và Bob thực hiện trao đổi thông tin với nhau, còn Trudy là kẻ xấu, đặt thiết bị can thiệp vào kênh truyền tin giữa Alice và Bob. Sau đây là các loại hành động tấn công của Trudy mà ảnh hưởng đến quá trình truyền tin giữa Alice và Bob:

- 1) **Xem trộm thông tin (Release of Message Content):** Trong trường hợp này Trudy chặn các thông điệp Alice gửi cho Bob, và xem được nội dung của thông điệp.

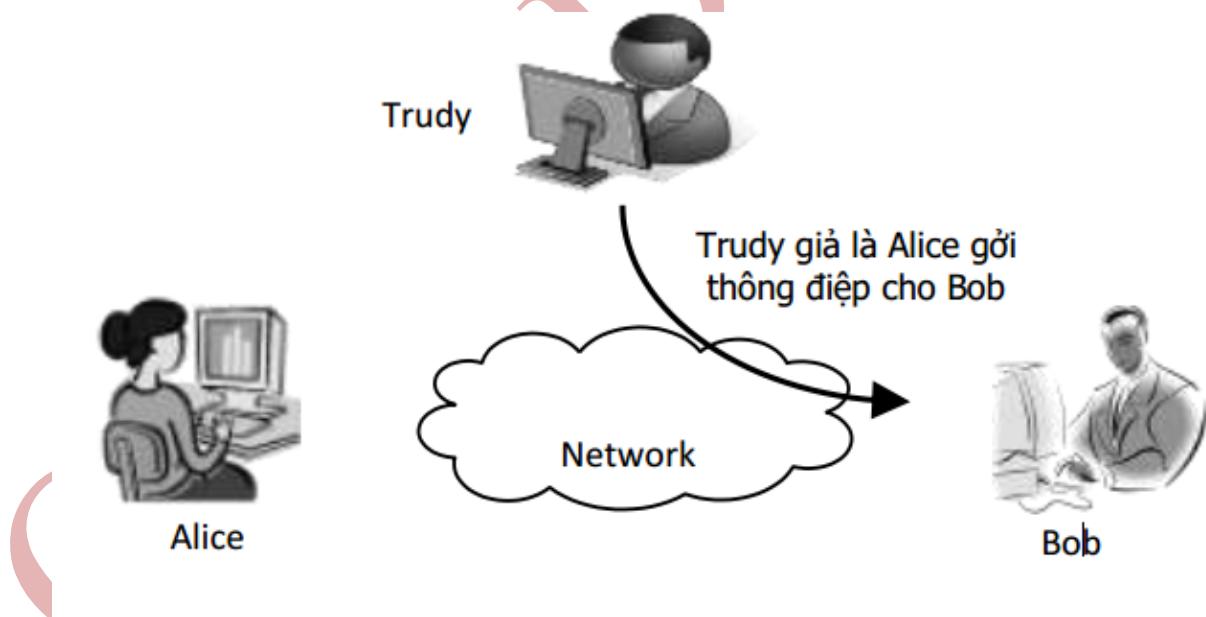


- 2) **Thay đổi thông điệp (Modification of Message):** Trudy chặn các thông điệp Alice gửi cho Bob và ngăn không cho các thông điệp này đến đích. Sau đó Trudy thay đổi nội dung của thông điệp và gửi tiếp cho Bob. Bob nghĩ rằng nhận được thông điệp nguyên bản ban đầu của Alice mà không biết rằng chúng đã bị sửa đổi.



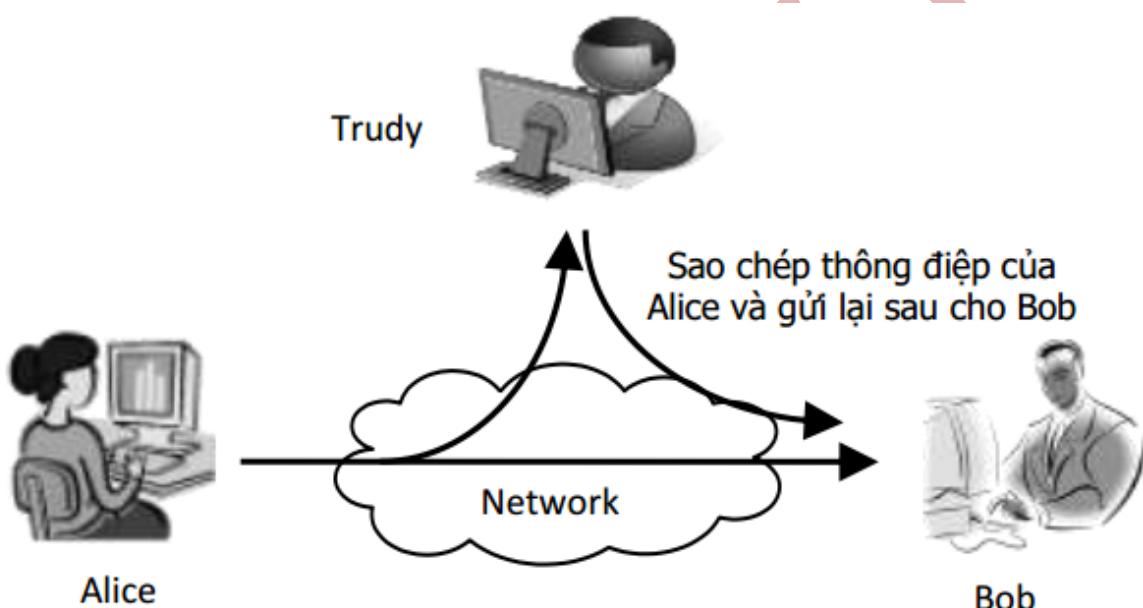
### 3) Mạo danh (Masquerade)

Trong trường hợp này Trudy giả là Alice gửi thông điệp cho Bob. Bob không biết điều này và nghĩ rằng thông điệp là của Alice.



**Hình 1-3. Mạo danh**

**4) Phát lại thông điệp (Replay):** Trudy sao chép lại thông điệp Alice gửi cho Bob. Sau đó một thời gian Trudy gửi bản sao chép này cho Bob. Bob tin rằng thông điệp thứ hai vẫn là từ Alice, nội dung hai thông điệp là giống nhau. Thoạt đầu có thể nghĩ rằng việc phát lại này là vô hại, tuy nhiên trong nhiều trường hợp cũng gây ra tác hại không kém so với việc giả mạo thông điệp. Xét tình huống sau: giả sử Bob là ngân hàng còn Alice là một khách hàng. Alice gửi thông điệp đề nghị Bob chuyển cho Trudy 1000\$. Alice có áp dụng các biện pháp như chữ ký điện tử với mục đích không cho Trudy mạo danh cũng như sửa thông điệp. Tuy nhiên nếu Trudy sao chép và phát lại thông điệp thì các biện pháp bảo vệ này không có ý nghĩa. Bob tin rằng Alice gửi tiếp một thông điệp mới để chuyển thêm cho Trudy 1000\$ nữa.



### Yêu cầu của một hệ truyền thông tin an toàn và bảo mật

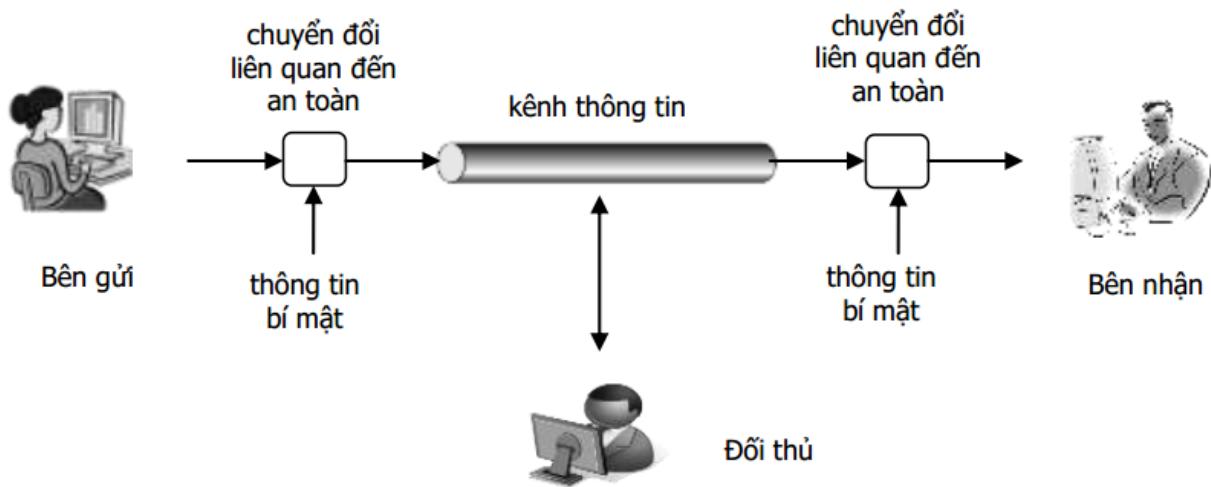
Phần trên đã trình bày các hình thức tấn công, một hệ truyền tin được gọi là an toàn và bảo mật thì phải có khả năng chống lại được các hình thức tấn công trên. Như vậy hệ truyền tin phải có các đặc tính sau:

- **Tính bảo mật** (Confidentiality): Ngăn chặn được vấn đề xem trộm thông điệp.
- **Tính chứng thực** (Authentication): Nhằm đảm bảo cho Bob rằng thông điệp mà Bob nhận được thực sự được gửi đi từ Alice, và không bị thay đổi trong quá trình truyền.

tin. Như vậy tính chứng thực ngăn chặn các hình thức tấn công sửa thông điệp, mạo danh, và phát lại thông điệp.

- **Tính không từ chối** (Nonrepudiation): xét tình huống sau: Giả sử Bob là nhân viên môi giới chứng khoán của Alice. Alice gửi thông điệp yêu cầu Bob mua cổ phiếu của công ty Z. Ngày hôm sau, giá cổ phiếu công ty này giảm hơn 50%. Thấy bị thiệt hại, Alice nói rằng Alice không gửi thông điệp nào cả và quy trách nhiệm cho Bob. Bob phải có cơ chế để xác định rằng chính Alice là người gửi mà Alice không thể từ chối trách nhiệm được.

Khái niệm chữ ký trên giấy mà con người đang sử dụng ngày nay là một cơ chế để bảo đảm tính chứng thực và tính không từ chối. Và trong lĩnh vực máy tính, người ta cũng thiết lập một cơ chế như vậy, cơ chế này được gọi là chữ ký điện tử.



### Vai trò của mật mã trong việc bảo mật thông tin trên mạng

Mật mã hay mã hóa dữ liệu (cryptography), là một công cụ cơ bản thiết yếu của bảo mật thông tin. Mật mã đáp ứng được các nhu cầu về tính bảo mật (confidentiality), tính chứng thực (authentication) và tính không từ chối (non-repudiation) của một hệ truyền tin. Tài liệu này trước tiên trình bày về mật mã cổ điển. Những hệ mật mã cổ điển này tuy ngày nay tuy ít được sử dụng, nhưng chúng thể hiện những nguyên lý cơ bản được ứng dụng trong mật mã hiện đại. Dựa trên nền tảng đó, chúng ta sẽ tìm hiểu về mã hóa đối xứng và mã hóa bất đối xứng, chúng đóng vai trò quan trọng trong mật mã hiện đại. Bên cạnh đó

chúng ta cũng sẽ tìm hiểu về hàm Hash, cũng là một công cụ bảo mật quan trọng mà có nhiều ứng dụng lý thú, trong đó có chữ ký điện tử.

## Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

Ngày nay, khi mạng Internet đã kết nối các máy tính ở khắp nơi trên thế giới lại với nhau, thì vấn đề bảo vệ máy tính khỏi sự thâm nhập phá hoại từ bên ngoài là một điều cần thiết. Thông qua mạng Internet, các hacker có thể truy cập vào các máy tính trong một tổ chức (dùng telnet chẳng hạn), lấy trộm các dữ liệu quan trọng như mật khẩu, thẻ tín dụng, tài liệu... Hoặc đơn giản chỉ là phá hoại, gây trực trặc hệ thống mà tổ chức đó phải tốn nhiều chi phí để khôi phục lại tình trạng hoạt động bình thường.

Để thực hiện việc bảo vệ này, người ta dùng khái niệm “kiểm soát truy cập” (Access Control). Khái niệm kiểm soát truy cập này có hai yếu tố sau:

+ Chứng thực truy cập (Authentication): xác nhận rằng đối tượng (con người hay chương trình máy tính) được cấp phép truy cập vào hệ thống. Ví dụ: để sử dụng máy tính thì trước tiên đối tượng phải logon vào máy tính bằng username và password. Ngoài ra, còn có các phương pháp chứng thực khác như sinh trắc học (dấu vân tay, mống mắt...) hay dùng thẻ (thẻ ATM...).

+ Phân quyền (Authorization): các hành động được phép thực hiện sau khi đã truy cập vào hệ thống. Ví dụ: bạn được cấp username và password để logon vào hệ điều hành, tuy nhiên bạn chỉ được cấp quyền để đọc một file nào đó. Hoặc bạn chỉ có quyền đọc file mà không có quyền xóa file. Với nguyên tắc như vậy thì một máy tính hoặc một mạng máy tính được bảo vệ khỏi sự thâm nhập của các đối tượng không được phép. Tuy nhiên thực tế chúng ta vẫn nghe nói đến các vụ tấn công phá hoại. Để thực hiện điều đó, kẻ phá hoại tìm cách phá bỏ cơ chế Authentication và Authorization bằng các cách thức sau:

+ Dùng các đoạn mã phá hoại (Malware): như virus, worm, trojan, backdoor...những đoạn mã độc này phát tán lan truyền từ máy tính này qua máy tính khác dựa trên sự bất cẩn của người sử dụng, hay dựa trên các lỗi của phần mềm. Lợi dụng các quyền được cấp cho người sử dụng (chẳng hạn rất nhiều người login vào máy tính với quyền administrator), các

đoạn mã này thực hiện các lệnh phá hoại hoặc dò tìm password của quản trị hệ thống để gửi cho hacker, cài đặt các cổng hậu để hacker bên ngoài xâm nhập

+ Thực hiện các hành vi xâm phạm (Intrusion): việc thiết kế các phần mềm có nhiều lỗ hổng, dẫn đến các hacker lợi dụng để thực hiện những lệnh phá hoại. Những lệnh này thường là không được phép đối với người bên ngoài, nhưng lỗ hổng của phần mềm dẫn đến được phép. Trong những trường hợp đặc biệt, lỗ hổng phần mềm cho phép thực hiện những lệnh phá hoại mà ngay cả người thiết kế chương trình không ngờ tới. Hoặc hacker có thể sử dụng các cổng hậu do các backdoor tạo ra để xâm nhập.

Để khắc phục các hành động phá hoại này, người ta dùng các chương trình có chức năng gác cổng, phòng chống. Những chương trình này dò tìm virus hoặc dò tìm các hành vi xâm phạm để ngăn chặn chúng, không cho chúng thực hiện hoặc xâm nhập. Đó là các chương trình chống virus, chương trình firewall... Ngoài ra các nhà phát triển phần mềm cần có quy trình xây dựng và kiểm lỗi phần mềm nhằm hạn chế tối đa những lỗ hổng bảo mật có thể có.

## 2.2 Lỗ hổng bảo mật và phương pháp phát hiện

Tất cả những đặc tính của phần mềm hay phần cứng mà cho phép người dùng không hợp lệ, có thể truy cập hay tăng quyền truy nhập mà không cần xác thực. Xét trên phương diện tổng quát: lỗ hổng là tất cả mọi yếu tố mà kẻ tấn công có thể lợi dụng để xâm nhập vào hệ thống.

**Có 3 loại lỗ hổng bảo mật:**

- Lỗ hổng làm cho từ chối dịch vụ: Cho phép hacker lợi dụng làm tê liệt một số dịch vụ của hệ thống. Với việc tấn công lỗ hổng làm từ chối dịch vụ, kẻ tấn công có thể làm mất khả năng hoạt động của máy tính hay một mạng, ảnh hưởng tới toàn bộ tổ chức công ty. Lỗ hổng bảo mật làm từ chối dịch vụ chia ra làm ba loại:
  - Bandwidth/Throughput Attacks
  - Protocol Attacks
  - Software Vulnerability Attacks

- Lỗi hổng cho phép tăng quyền của người dùng không xác thực: Là lỗi hổng cho phép người dùng bên trong mạng với quyền hạn chế có thể tăng quyền mà không cần xác thực. Lỗi này xuất hiện ở những phần mềm hay hệ điều hành có sự phân cấp người dùng. Cho phép loại người dùng với mức sử dụng hạn chế có thể tăng quyền trái phép.

Ví dụ : cho phép người dùng bình thường có thể khởi động tiến trình sendmail, lợi dụng sendmail khởi động chương trình khác với quyền root

- Lỗi hổng cho xâm nhập từ xa không xác thực.

Là loại lỗi hổng bảo mật cho phép kẻ không phải là người dùng hệ thống có thể xâm nhập từ xa không xác thực. Lỗi gây ra lỗi hổng bảo mật này thường là lỗi chủ quan của người quản trị hệ thống hay người dùng. Do không thận trọng, thiếu kinh nghiệm, và không quan tâm đến vấn đề bảo mật. Một số biểu hiện thường gặp của loại lỗi hổng bảo mật này là: Tài khoản có password rỗng, tài khoản mặc định, không có hệ thống bảo vệ, chạy những dịch vụ không cần thiết mà không an toàn: SNMP, pcAnywhere, VNC , ...

Một số lỗi hổng trên quan điểm ứng dụng:

- Lỗi phần mềm, chẳng hạn như Microsoft Office, Java, Flash Player, QuickTime.
- Các tập tin tạm thời của một chương trình được cài đặt hoặc cập nhật, hoặc cập nhật Windows.

### **Lỗi phần mềm**

Ngay cả những phần mềm tầm trung đơn giản, chỉ phục vụ một vài tác vụ chuyên biệt cũng đã tạo thành từ một lượng lớn code. Cấu trúc phần mềm được thiết kế bởi con người, và những dòng code trong đó cũng được viết bởi con người, vì vậy việc xuất hiện lỗi là không thể tránh khỏi. Trong phần lớn trường hợp, nếu một phần mềm được sản xuất một cách chuyên nghiệp – các lỗi này không thể có tác động gì quá lớn, nhất là đến các khía cạnh về bảo mật. Cùng lăm ta sẽ thấy một vài chức năng không hoạt động, đôi lúc phần mềm “treo” khi đang làm việc hoặc làm việc chậm chạp... Nhưng nói vậy không có nghĩa là những lỗi nghiêm trọng liên quan đến bảo mật không thể xảy ra. Nói cụ thể hơn một chút, đó là những lỗi phần mềm mà người ngoài có thể khai thác để tác động thay đổi cách phần mềm vận hành, đưa thêm vào các đoạn mã tự viết, xem các dữ liệu mà phần mềm quản lí...

Ngoài các nguyên nhân chủ quan như sự bất cẩn khi sử dụng của người dùng (click vào đường link lạ, download các phần mềm độc hại), các lỗi này là một trong những khe hở chính mà tin tặc thường tập trung khai thác để xâm nhập vào các hệ thống máy móc – từ các máy chủ đến các máy cá nhân của người dùng cuối. Nếu lỗi hỏng này thuộc về một phần mềm không phổ biến, chỉ phục vụ vài tác vụ đơn giản và không có vai trò quan trọng trong hệ thống, hiển nhiên hiểm họa về bảo mật vẫn có nhưng không nghiêm trọng. Nhưng hệ thống phần mềm càng phức tạp, đồ sộ thì hiển nhiên việc kiểm soát sự xuất hiện của những lỗi này càng khó – bất kể các kỹ sư thiết kế có trình độ cao đến đâu. Và chính những phần mềm này lại thường chiếm vai trò chủ chốt, cũng như tác động đến nhiều ngóc ngách của hệ thống. Nhờ len lỏi qua kẽ hở tạo ra bởi lỗi của những phần mềm này, kẻ xấu có thể thực hiện những thay đổi nhất định lên máy móc của người dùng, hay nắm được quyền điều khiển, truy cập các thông tin nhạy cảm.

## **Zero-Day Exploits – Đòn tấn công âm thầm**

Thực tế, các lỗi hỏng có thể bị khai thác sử dụng cho mục đích xấu tàn tại trên bất cứ phần mềm nào. Thậm chí có những phần của thiết kế khó có thể bị cho là lỗi cho đến khi xuất hiện những công nghệ cho phép người ngoài khai thác nó – khiến cho tác giả phải thiết kế lại cách sản phẩm của mình vận hành. Khi cập nhật phần mềm mới, ngoài việc đôi lúc thấy xuất hiện các chức năng mới, hay hiệu năng hoạt động được cải thiện, chắc hẳn không ít lần bạn thấy changelog(danh sách các thay đổi) xuất hiện một loạt các sửa chữa lỗi gần đây nhất. Những người tạo ra một sản phẩm dĩ nhiên phải là người hiểu rõ đúra con cưng của mình nhất – và sẽ cố hết sức để sửa chữa lỗi mỗi khi phát hiện ra (ít nhất thì phần lớn trường hợp là như vậy). Với sản phẩm phổ biến trên thị trường, được phát hành bởi các công ty- tổ chức hoạt động một cách chuyên nghiệp, điều này càng đúng hơn.

Nhưng không có gì là tuyệt đối. Sẽ có những lúc mà tác giả phát hiện lỗi sau người ngoài, hoặc thậm chí là không đủ khả năng phát hiện ra. Không phải bỗng nhiên mà các hãng lớn thường tổ chức những cuộc thi về khai thác lỗi hỏng trên sản phẩm của mình, đồng thời tuyển mộ nhân lực từ các cuộc thi đó, cũng như tuyển mộ các tin tặc hoàn lương. Thực tế vẫn luôn như vậy: có người có tài, có người không. Thậm chí sẽ có những lúc hãng sản xuất phát hiện lỗi, nhưng thời gian để hoàn thành việc sửa chữa lại lâu hơn thời gian tin tặc

cần để viết ra công cụ khai thác, đồng thời hoàn thành công việc phá hoại, gián điệp hay trộm cắp bằng công cụ đó. Đó cũng là một trong những lí do khiến ta thấy các bài viết về lỗ hổng bảo mật thường chỉ xuất hiện nhiều tháng sau khi lỗi đã được sửa. Các hacker mũ trắng quá hiểu rằng việc sửa lỗi đôi lúc khó khăn và phức tạp hơn nhiều lần so với việc lợi dụng lỗi cho mục đích xấu, vì vậy họ thường cho hãng sản xuất hàng tháng trời để sửa chữa sai lầm của mình trước khi công bố chi tiết về lỗ hổng mà mình phát hiện ra ngoài để phục vụ mục đích nghiên cứu.

Còn kịch bản xấu nhất? Kẻ xấu phát hiện ra lỗi... và dĩ nhiên là không công bố cho ai biết, âm thầm đóng cửa tu luyện để hoàn thành công cụ khai thác lỗi và âm thầm phát tán (thường thấy nhất là dưới dạng virus, worm,trojan...). Thậm chí giới tội phạm có thể đem những thông tin này ra giao dịch, trao đổi ngầm với nhau, hay bán kèm trong những bộ kit được viết ra chuyên để phục vụ việc tìm hiểu, khai thác lỗ hổng. Hàng sản xuất hoàn toàn không biết sự tồn tại của lỗ hổng đó chứ đừng nói đến việc tìm cách sửa. Chỉ đến khi hậu quả đã sờ sờ ra trước mắt, họ mới có thể tá hỏa lên tìm cách khắc phục, đèn bù cho người dùng, như vụ việc của Sony ngày trước. Cũng chính vì đòn tấn công được thực hiện khi hãng sản xuất hoàn toàn chưa biết đến sự tồn tại của các lỗ hổng này, có "0 ngày" để tìm cách vá lỗi mà cái tên "zero-day" ra đời.

Tóm lại, việc một lỗi phần mềm tồn tại vốn không phải việc gì quá kì lạ, hiểm họa chỉ xuất hiện khi hãng sản xuất thua trong cả 2 cuộc đua: phát hiện lỗi và sửa lỗi.

### Quá trình khai thác

Cần hiểu rằng, các công cụ về bảo mật hiện đại ngày nay như tường lửa, phần mềm anti-virus, anti-malware... thường có cơ chế hoạt động thông minh để phát hiện khi một đoạn mã nào đó có hành vi đáng ngờ, bất kể đoạn mã đó có sẵn trong cơ sở dữ liệu về virus, malware hay không. Cũng tương tự như một trình sát dày dạn có thể phát hiện dấu hiệu khả nghi của một kẻ trộm mà không cần lệnh truy nã hay chữ "trộm" to đùng trước trán. Tuy vậy như đã nói, trường hợp xấu nhất là khi các tin tức phát hiện lỗi chưa ai biết tới, viết một công cụ hoàn toàn mới để khai thác. Một kẻ nếu đủ khả năng để về đích đầu tiên trong cả 2 cuộc đua này (ở đây không nói đến những đối tượng sử dụng lại công cụ) hẳn nhiên thừa

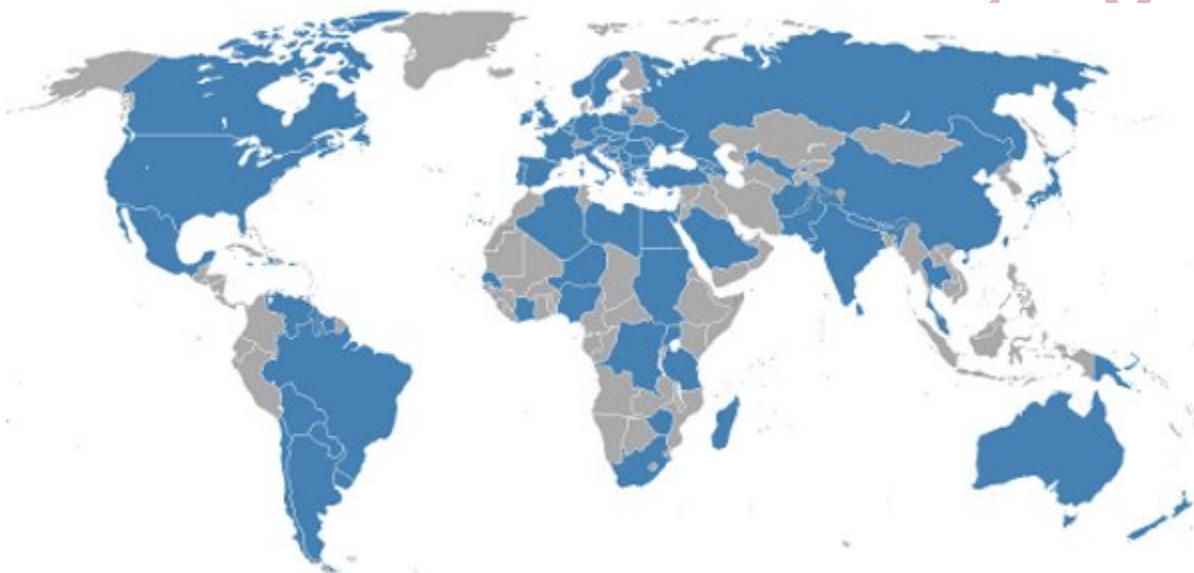
kinh nghiệm trong việc tránh ánh mắt dò xét của các công cụ bảo mật. Vì vậy cho đến khi lỗ hổng hoàn toàn được vá, mọi biện pháp mà các công cụ bảo mật cung cấp đều chỉ mang tính tạm thời. Chuỗi sự kiện điển hình thường là như sau:

1. Xuất hiện một lỗ hổng có thể bị khai thác bằng các công nghệ hiện có.
2. Kẻ tấn công phát hiện lỗ hổng.
3. Kẻ này lập tức tiến hành viết và phát tán công cụ khai thác lỗ hổng này.
4. Hàng sản xuất đồng thời phát hiện lỗi và lập tức tìm cách sửa chữa.
5. Lỗ hổng được công bố ra ngoài.
6. Các phần mềm anti-virus được cập nhật thông tin để phát hiện khi có các đoạn mã tìm cách khai thác lỗ hổng này.
7. Hàng sản xuất hoàn thành bản vá.
8. Hàng hoàn tất phát hành bản vá lỗi đến tất cả khách hàng.

Thời điểm của đợt tấn công đầu tiên hiển nhiên nằm giữa bước 3 và 5. Theo một nghiên cứu mới đây của đại học Carnegie Mellon của Mỹ, giai đoạn này trung bình kéo dài 10 tháng. Tuy nhiên không phải lúc nào tất cả người dùng cuối cũng bị nguy hiểm trong giai đoạn này. Dạng tấn công tận dụng thời điểm hàng sản xuất chưa phát hiện (hoặc chưa sửa được lỗi) này có lợi thế lớn nhất là sự kín đáo – phù hợp cho việc lấy trộm thông tin hoặc phá hoại ngầm mà không bị phát hiện. Vì vậy giai đoạn này đối tượng bị nhắm đến thường là một nhóm người có thể đem lại lợi ích cụ thể cho kẻ tấn công để sau đó hắn có thể rút đi êm thầm. Mục tiêu đó có thể là các tổ chức, tập đoàn mà kẻ này muốn phá hoại hoặc các thông tin tài khoản có thể sử dụng để kiếm lời.

Giai đoạn từ bước 5 đến 8 mới thực sự nguy hiểm. Đây là lúc thông tin về lỗ hổng được công bố, và cùng với các công ty phát triển anti-virus, những tin tức chưa biết đến lỗi này cũng có thể tiếp cận được thông tin. Làn sóng tấn công lúc này không còn âm thầm, mà dồn dập hơn rất nhiều. Nếu ví đợt tấn công trước đó nguy hiểm như một nhát dao đâm sau lưng, thì đợt tấn công lúc này như một chuỗi đòn đánh trực diện, không hiệu quả với những

ai cẩn thận đề phòng nhưng vẫn không kém phần nguy hiểm nếu như gặp đúng những người lơ là bảo mật hoặc nhỡ sử dụng công cụ bảo mật kém chất lượng, cập nhật chậm. Những đối tượng không có khả năng phát hiện lỗi, cũng như không có khả năng phát triển công cụ cũng tham gia từ thời điểm này, khiến việc phát tán và tìm đến những cỗ máy có hệ thống bảo mật yếu kém nhanh hơn rất nhiều. Khi số lượng kẻ tham gia tấn công tăng lên, động cơ và phương thức tấn công cũng đa dạng hơn chứ không thể chỉ thuần túy là len lỏi và trộm cắp nữa.



Sau khi đọc đến đây, chắc bạn đọc cũng hiểu rằng, khi nói đến việc bảo vệ thông tin và hệ thống của mình, ngoài việc cập nhật các biện pháp phòng thủ thì việc cập nhật thông tin cũng quan trọng không kém. Thường thì những lỗi nghiêm trọng của những hệ thống phổ biến và quan trọng như Java vừa qua sẽ được báo chí đăng tải nhanh chóng khi hãng sản xuất công bố. Tuy nhiên những phần mềm có danh tiếng và độ phổ biến “khiêm tốn” hơn thì thường không được ưu ái như vậy. Vì vậy ngoài việc chú ý nâng cấp bản vá lỗi, cần dừng việc sử dụng những phần mềm cũ kĩ không còn được chăm sóc, sửa lỗi ngay khi có thể. Ví dụ? Microsoft vẫn không ngừng kêu gào để những XP, IE6 được yên nghỉ đãi thôi...

### 2.3 Bảo mật đường truyền tải

Ngày nay, mọi mô hình truyền dữ liệu trên không gian mạng, người ta đều áp dụng những chuẩn giao thức về an toàn thông tin. Những giao thức này sẽ mã hóa toàn bộ thông

tin chuyển đi và đảm bảo dữ liệu không bị chỉnh sửa hoặc can thiệp trên đường truyền, dữ liệu đến đích luôn đảm bảo tính toàn vẹn

Một số giao thức bảo mật mạng như

- SSL
- TLS
- IPSec trong VPN
- Giao thức bảo mật mạng cục bộ Kerberos

Chúng ta sẽ nghiên cứu kỹ về chúng trong những chương sau hoặc trong một môn học chuyên ngành về lĩnh vực này

## 2.4 Bảo mật mạng không dây

### 2.4.1 WAP

WAP (viết tắt của Wireless Application Protocol - Giao thức Ứng dụng Không dây) là một tiêu chuẩn công nghệ cho các hệ thống truy nhập Internet từ các thiết bị di động như điện thoại di động, Smartphone. Mặc dù tiêu chuẩn này chưa được chuẩn hóa trên toàn cầu, nhưng những ứng dụng của giao thức này đã tác động rất lớn đến ngành công nghiệp di động và các lĩnh vực dịch vụ liên quan. WAP là giao thức truyền thông mang lại rất nhiều ứng dụng cho người sử dụng thiết bị đầu cuối di động như E-mail, web, mua bán trực tuyến, ngân hàng trực tuyến, thông tin chứng khoán.

Với các xu hướng triển khai các ứng dụng vô tuyến băng thông rộng trong mạng NGN, rất nhiều các công nghệ đã được đề xuất để tích hợp và hội tụ các dịch vụ mạng. WAP là một giải pháp công nghệ đem lại nhiều lợi ích cho người sử dụng thiết bị đầu cuối vô tuyến cũng như các giá trị tăng của các nhà cung cấp dịch vụ mạng. Tuy nhiên, triển khai WAP là một vấn đề phức tạp và liên quan tới nhiều hướng phát triển công nghệ khác như phần cứng, bảo mật và các vấn đề khác.

WAP ứng dụng ngôn ngữ WML để triển khai và thể hiện các trang web tiêu chuẩn cho phù hợp với các thiết bị di động. Sử dụng khuôn dạng tín hiệu dữ liệu tối ưu, WAP được thiết kế để duyệt các nội dung web tới thiết bị vô tuyến thông qua loại bỏ các thành

phần đồ họa nhằm hiển thị trên màn hình nhỏ và hạn chế băng thông. Thực tế rất nhiều mã WML được sửa đổi từ mã HTML.

Mặc dù WAP hỗ trợ cho hầu hết các thiết bị di động nhưng nó vẫn tồn tại một số điểm hạn chế trong giao thức này:

- Độ trễ: WAP dựa trên giao thức TCP/IP và không tự xây dựng hệ thống bảo mật riêng cũng như khả năng tự đẩy dữ liệu, điều này sẽ ảnh hưởng tới những ứng dụng cần được chạy ngay khi người dùng đang truyền dữ liệu trên một ứng dụng khác. Nếu triển khai ứng dụng kiểu này sẽ tăng độ phức tạp của hệ thống lên rất lớn và ảnh hưởng trực tiếp tới phần cứng và băng thông yêu cầu.
- Bảo mật: WAP là hệ thống giao thức điển hình không chứa bảo mật riêng, điều đó có nghĩa là dữ liệu không được mã hoá khi truyền. Các phần mềm bảo mật có thể được hỗ trợ cho WAP nhưng bị giới hạn vì độ ổn định, giá thành và thời gian thực hiện. Gateway: Giải pháp WAP yêu cầu có gateway vô tuyến, vì vậy nó sẽ làm tăng giá thành của hệ thống.
- Kết nối liên tục: Các ứng dụng WAP được xây dựng dựa trên kiến trúc yêu cầu/ đáp ứng vì vậy nó sẽ kết nối liên tục không giống như trên các trình duyệt trên các máy PC. Một số người sử dụng thường di chuyển vượt qua vùng phủ sóng và gây ra các lỗi kết nối. Vấn đề này có thể giải quyết bằng phương pháp "lưu và chuyển tiếp", giải pháp thêm vào này cũng làm tăng giá thành và độ phức tạp của hệ thống. Trên thực tế, việc thêm vào khả năng yêu cầu phản ứng kèm theo và tăng thêm băng thông sử dụng.
- Triển khai dịch vụ: WAP được tạo ra để duyệt nội dung các trang web, các nhà cung cấp nội dung được yêu cầu quản lý và duy trì các bản sao cho mỗi website. Các bản sao như vậy thực sự là không hiệu quả vì nó làm tăng giá thành khi mở rộng và bảo dưỡng hệ thống.
- Tương tác thấp: WAP rất khó tích hợp với các ứng dụng có sẵn trên các thiết bị, đây là giới hạn thường thấy của các giải pháp trên các đầu cuối có năng lực xử lý và giao diện màn hình nhỏ.

- **Khả năng đẩy và kéo:** Các giải pháp WAP yêu cầu người sử dụng gửi các thông tin trước khi họ nhận chúng, Như vậy, email, cảnh báo không thể nhận ngay tức khắc. Thuật ngữ "kéo" liên quan tới khả năng của thiết bị để cảnh báo người sử dụng khi có dữ liệu của họ đến. Chức năng đẩy là chức năng có sẵn của WAP nhưng nó yêu cầu thêm một lớp kiến trúc và như vậy sẽ làm tăng nguy cơ xảy ra lỗi và trễ.

#### 2.4.2 WEP

Wired Equivalent Privacy (WEP) là thuật toán bảo mật WiFi được dùng nhiều nhất trên thế giới. Thực tế nó là thứ đầu tiên xuất hiện trong menu các chuẩn mã hóa của nhiều bộ định tuyến.

WEP được phê chuẩn là phương thức bảo mật tiêu chuẩn dành cho WiFi vào tháng 9/1999. Phiên bản đầu tiên của WEP không hề mạnh, kể cả vào thời điểm nó được giới thiệu bởi việc chính phủ Mỹ cấm xuất khẩu nhiều công nghệ mã hóa khiến các nhà sản xuất chỉ bảo vệ thiết bị của họ với mã hóa 64 bit. Sau khi lệnh cấm được dỡ bỏ, chuẩn 128 bit được đưa vào sử dụng rộng rãi hơn. Thậm chí sau này kể cả khi mã hóa WEP 256 bit được giới thiệu, 128 bit vẫn là một trong những chuẩn được áp dụng nhiều nhất.

Mặc dù các thuật toán được cải tiến và kích thước kí tự được tăng lên, qua thời gian nhiều lỗ hổng bảo mật được phát hiện trong chuẩn WEP khiến nó càng ngày càng dễ bị qua mặt khi mà sức mạnh của máy tính ngày càng được củng cố. Năm 2001, nhiều lỗ hổng tiềm tàng đã bị phơi bày trên mạng Internet. Đến năm 2005, FBI công khai trình diễn khả năng bẻ khóa WEP chỉ trong một vài phút bằng phần mềm hoàn toàn miễn phí nhằm nâng cao nhận thức về sự nguy hiểm của WEP.

Mặc dù nhiều nỗ lực cải tiến được tiến hành nhằm tăng cường hệ thống của WEP, chuẩn này vẫn đặt người dùng vào vị trí hết sức nguy hiểm và tất cả các hệ thống sử dụng WEP nên được nâng cấp hoặc thay thế. Tổ chức Liên minh WiFi chính thức cho WEP "về hưu" năm 2004.

#### 2.4.3 WPA,WPA2

WiFi Protected Access là phương thức được Liên minh WiFi đưa ra để thay thế WEP trước những nhược điểm không thể khắc phục của chuẩn cũ. WPA được áp dụng chính thức

vào năm 2003, một năm trước khi WEP bị loại bỏ. Phiên bản phổ biến nhất của WPA là WPA-PSK (Pre-Shared Key). Các kí tự được sử dụng bởi WPA là loại 256 bit, tân tiến hơn rất nhiều so với kí tự 64 bit và 128 bit có trong hệ thống WEP.

Một trong những thay đổi lớn lao được tích hợp vào WPA bao gồm khả năng kiểm tra tính toàn vẹn của gói tin (message integrity check) để xem liệu hacker có thu thập hay thay đổi gói tin chuyền qua lại giữa điểm truy cập và thiết bị dùng WiFi hay không. Ngoài ra còn có giao thức khóa toàn vẹn thời gian (Temporal Key Integrity Protocol – TKIP). TKIP sử dụng hệ thống kí tự cho từng gói, an toàn hơn rất nhiều so với kí tự tĩnh của WEP. Sau này, TKIP bị thay thế bởi Advanced Encryption Standard (AES).

Tuy vậy điều này không có nghĩa là WPA đã hoàn hảo. TKIP, một bộ phận quan trọng của WPA, được thiết kế để có thể tung ra thông qua các bản cập nhật phần mềm lên thiết bị được trang bị WEP. Chính vì vậy nó vẫn phải sử dụng một số yếu tố có trong hệ thống WEP, vốn cũng có thể bị kẻ xấu khai thác.

WPA, giống như WEP, cũng trải qua các cuộc trình diễn công khai để cho thấy những yếu điểm của mình trước một cuộc tấn công. Phương pháp qua mặt WPA không phải bằng cách tấn công trực tiếp vào thuật toán của nó mà là vào một hệ thống hỗ trợ có tên WiFi Protected Setup (WPS), được thiết kế để có thể dễ dàng kết nối thiết bị tới các điểm truy cập.

## **WPA2 viết tắt của WiFi Protected Access II**

Đến năm 2006, WPA chính thức bị thay thế bởi WPA2. Một trong những cải tiến đáng chú ý nhất của WPA2 so với WPA là sự có mặt bắt buộc của AES và CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) nhằm thay thế cho TKIP. Tuy vậy, TKIP vẫn có mặt trong WPA2 để làm phương án dự phòng và duy trì khả năng tương tác với WPA.

Hiện tại, lỗ hổng bảo mật chính của hệ thống WPA2 không thực sự rõ. Kẻ tấn công phải có quyền truy cập vào mạng WiFi đã được bảo vệ trước khi có thể có trong tay bộ kí tự, sau đó mới có thể tiến hành tấn công các thiết bị khác trong cùng mạng. Như vậy, các

lỗ hổng của WPA2 khá hạn chế và gần như chỉ gây ảnh hưởng đến các mạng quy mô lớn như của tập đoàn. Trong khi đó người dùng mạng tại nhà có thể yên tâm với chuẩn mới nhất này.

Tuy nhiên không may là lỗ hổng lớn nhất trong bộ giáp của WPA vẫn còn tồn tại trong WPA2, đó là WPS. Mặc dù để thâm nhập được vào mạng lưới được bảo vệ bởi WPA/WPA2 bằng lỗ hổng trên cần tới 2-14 giờ hoạt động liên tục của một máy tính hiện đại, đây vẫn là một mối lo tiềm tàng. Vì thế tốt nhất WPS nên được tắt đi hoặc xóa bỏ hoàn toàn khỏi hệ thống thông qua các lần cập nhật firmware của điểm truy cập.

Dưới đây là danh sách các chuẩn bảo mật dành cho WiFi, xếp theo khả năng bảo mật từ cao xuống thấp:

- ✓ WPA2 + AES
- ✓ WPA + AES
- ✓ WPA + TKIP/AES (TKIP đóng vai trò là phương án dự phòng)
- ✓ WPA + TKIP
- ✓ WEP
- ✓ Mạng mở, không mã khóa

## 2.5 Bảo mật thư điện tử

Để thông tin email truyền đi an toàn, ngày nay người ta thường dùng nhiều kỹ thuật và giao thức, quy trình xác thực khác nhau như PGP. Chi tiết về bảo mật thư điện tử sẽ được trình bày kỹ trong một môn học An toàn thư điện tử trong năm học kế tiếp.

## 2.6 An ninh mạng

### 2.6.1 Chính sách an ninh mạng

Vi phạm an ninh mạng có thể bắt đầu từ ngay bên trong một tổ chức và phụ thuộc nhiều vào lỗi của con người. Phần này trình bày cách để giảm thiểu các nguy cơ đột nhập bằng cách giao tiếp và quản lý người sử dụng trong tổ chức của bạn thông qua một chính sách an ninh đã được lên kế hoạch kỹ lưỡng.

Một chính sách an ninh (security policy) sẽ định rõ các mục tiêu an toàn bảo mật, nguy cơ, mức phân quyền, bổ nhiệm điều phối viên và các thành viên nhóm bảo mật, phân

trách nhiệm cho mỗi thành viên trong nhóm, và trách nhiệm của mỗi nhân viên. Ngoài ra, chính sách an ninh cũng quy định cụ thể cách giải quyết các vi phạm an toàn và bảo mật. Nó không cần đưa ra chính xác phần cứng, phần mềm, kiến trúc, hoặc các giao thức sẽ được sử dụng để đảm bảo an toàn, cũng không đưa ra cách phần cứng hoặc phần mềm sẽ được cài đặt và cấu hình như thế nào. Những chi tiết này thay đổi theo thời gian và cần được chia sẻ chỉ với quản trị mạng hoặc người quản lý có thẩm quyền.

## Mục tiêu của chính sách an ninh

Trước khi xây dựng một chính sách an ninh, bạn nên hiểu lý do tại sao các chính sách an ninh là cần thiết và chính sách đó sẽ có lợi cho tổ chức của bạn như thế nào. Các mục tiêu chính của chính sách an ninh như sau:

- ✓ Đảm bảo rằng người dùng hợp lệ có quyền truy cập đến các tài nguyên mà họ cần.
- ✓ Ngăn chặn người dùng trái phép truy cập vào mạng, các hệ thống, các chương trình, hoặc dữ liệu.
- ✓ Bảo vệ dữ liệu nhạy cảm từ các truy cập trái phép, cả từ bên trong và bên ngoài tổ chức.
- ✓ Ngăn chặn sự cố ngẫu nhiên cho phần cứng hoặc phần mềm.
- ✓ Ngăn chặn sự cố có chủ ý cho phần cứng hoặc phần mềm.
- ✓ Tạo một môi trường mà các mạng và hệ thống có thể chịu được, và nếu cần thiết, nhanh chóng đáp ứng và phục hồi lại từ bất kỳ mối đe dọa nào.
- ✓ Truyền thông tới các nhân viên về trách nhiệm trong việc duy trì tính toàn vẹn dữ liệu và bảo mật hệ thống.

Chính sách an ninh của một công ty không chỉ liên quan đến một máy tính hoặc mạng riêng. Ví dụ, nó có thể quy định rằng mỗi nhân viên phải hủy tập giấy có chứa dữ liệu nhạy cảm hoặc mỗi nhân viên chịu trách nhiệm đăng ký cho khách của mình tại quầy lễ tân và lấy thẻ ra vào tạm thời cho họ. Tuy nhiên, các chính sách an ninh không liên quan đến máy tính nằm ngoài phạm vi của môn học này

Sau khi xác định các mục tiêu của chính sách an ninh của công ty bạn, bạn có thể đưa ra chiến lược để đạt được chúng. Trước tiên, bạn có thể tổ chức một ủy ban gồm các nhà quản lý và bên quan tâm từ nhiều phòng ban khác nhau ngoài các quản trị mạng. Càng nhiều người ra quyết định có thể mời tham gia thì chính sách của bạn sẽ càng hiệu quả và được hỗ trợ nhiều hơn.

Ủy ban này có thể chỉ định ra một điều phối viên an ninh (security coordinator), người này sau đó sẽ thúc đẩy việc tạo ra một chính sách an ninh. Để tăng sự đồng thuận của chính sách an ninh trong tổ chức của bạn, ràng buộc các biện pháp an ninh với nhu cầu kinh doanh và chỉ rõ những ảnh hưởng của lỗ hổng an ninh. Ví dụ, nếu công ty của bạn bán quần áo trên mạng Internet và bị ngừng hai tiếng đồng hồ gây tổn thất tới doanh thu của công ty là 1 triệu đô, hãy làm cho người dùng và người quản lý hiểu được điều này. Từ đó, các nhà quản lý sẽ mong muốn nắm rõ chính sách an ninh hơn.

Một chính sách an ninh phải nhắm đến những rủi ro cụ thể của một tổ chức. Để hiểu những rủi ro của tổ chức, bạn nên tiến hành kiểm định an toàn, xác định các lỗ hổng và đánh giá mức độ nghiêm trọng của các mối đe dọa và khả năng xảy ra của nó như đã mô tả trong chương này. Sau khi xác định được các nguy cơ, điều phối viên an ninh nên chỉ định một người chịu trách nhiệm để giải quyết các mối đe dọa đó.

## Nội dung chính sách an ninh

Sau khi bạn đã xác định các nguy cơ và phân công trách nhiệm quản lý chúng, bạn sẽ tiến hành phác thảo nội dung của chính sách. Các nhóm phác thảo chính sách có thể bao gồm: chính sách về mật khẩu, chính sách cài đặt phần mềm, chính sách dữ liệu bí mật và nhạy cảm, chính sách truy cập mạng, chính sách sử dụng E-mail, chính sách sử dụng Internet, chính sách truy cập từ xa, các chính sách kết nối với mạng của khách hàng và của các nhà cung cấp, chính sách sử dụng smartphone và máy tính xách tay cá nhân, và chính sách sử dụng phòng máy. Mặc dù biên soạn tất cả các thông tin này có thể sẽ khó khăn, tuy nhiên quá trình này đảm bảo rằng mọi người hiểu quan điểm của tổ chức về an toàn và lý do tại sao nó quan trọng. Chính sách an ninh nên giải thích cho người dùng hiểu những gì họ có thể và không thể làm và điều đó bảo vệ an toàn mạng như thế nào. Phần quy định về

người dùng có thể sắp xếp các quy tắc bảo mật theo chức năng cụ thể hoặc theo phần của mạng mà họ sử dụng. Phương pháp này làm cho các chính sách an ninh dễ dàng đọc và hiểu hơn với người sử dụng, ngoài ra nó cũng giúp họ không phải đọc toàn bộ tài liệu. Ví dụ, trong “Mật khẩu”, các hướng dẫn có thể bao gồm: “Người dùng không chia sẻ mật khẩu với bạn bè hoặc thân”, “người sử dụng phải chọn mật khẩu có hơn mười ký tự và gồm cả chữ cái và chữ số”, và “người sử dụng nên chọn mật khẩu khác tên của vợ hoặc chồng, tên vật nuôi, ngày sinh, ngày kỷ niệm hoặc các thông tin phổ biến rộng rãi khác”.

Một chính sách an ninh cũng nên định rõ những thông tin có ý nghĩa bí mật của một tổ chức. Nhìn chung, thông tin mật là các thông tin có thể bị sử dụng bởi các bên khác để làm suy yếu hoạt động của tổ chức, làm giảm sự tín nhiệm của khách hàng, gây ra tổn thất tài chính, gây ảnh hưởng đến hoạt động của một tổ chức, hoặc mang lại lợi thế cho đối thủ cạnh tranh. Tuy nhiên, nếu bạn làm việc trong một môi trường bệnh viện với hầu hết các dữ liệu mang tính nhạy cảm hoặc bí mật, chính sách an ninh của bạn nên phân loại các thông tin theo mức độ nhạy cảm ứng với phân quyền sử dụng các thông tin đó. Ví dụ, dữ liệu tối mật chỉ được sử dụng bởi Giám đốc điều hành (CEO) hay các phó giám đốc của tổ chức, trong khi dữ liệu mật khác có thể được truy cập vào từ những người tạo ra và thay đổi dữ liệu đó (ví dụ: bác sĩ hay kế toán của bệnh viện). Chính sách phản ứng Cuối cùng, một chính sách an ninh cần phải có kế hoạch ứng phó trong các trường hợp bị tấn công. Chính sách phản ứng sẽ chỉ ra các thành viên của một đội phản ứng, trong đó tất cả các thành viên hiểu rõ về các chính sách an ninh, các sự cố và các biện pháp xử lý tại chỗ. Mỗi thành viên trong đội sẽ giữ một vai trò với trách nhiệm nhất định. Đội phản ứng an ninh mạng nên thường xuyên diễn tập phòng tránh tấn công bằng cách giả lập các cuộc tấn công.

### Vai trò đội có thể bao gồm:

- Điều phối viên – Người trực, anh ta là người đầu tiên thông báo hoặc được báo về sự cố. Người điều phối sẽ thông báo cho lãnh đạo các chuyên viên hỗ trợ kỹ thuật và sau đó là giám đốc. Đồng thời anh ấy cũng ghi chép lại sự việc, chi tiết về thời gian bắt đầu, các dấu của nó, và bắt cứ thông tin cần thiết về trường hợp này. Người điều phối luôn sẵn sàng trả lời các cuộc gọi từ các khách hàng hoặc các nhân viên hoặc hỗ trợ người quản lý.

- Người quản lý - Thành viên trong đội, người sẽ điều phối các nhân viên để giải quyết vấn đề. Nếu các kỹ thuật viên tại chỗ không thể xử lý bước đầu, người quản lý sẽ tìm sự hỗ trợ từ bên ngoài. Người quản lý cũng đảm bảo rằng chính sách an ninh được làm theo và tất cả mọi người trong tổ chức nhận thức được tình hình. Sau sự cố, người quản lý tiếp tục theo dõi các sự kiện và truyền tải lại với các chuyên viên quan hệ công chúng.
- Chuyên viên hỗ trợ kỹ thuật - Thành viên này của đội tập trung vào một nhiệm vụ duy nhất: Giải quyết vấn đề càng nhanh càng tốt. Sau khi tình hình đã được giải quyết, các chuyên viên hỗ trợ kỹ thuật mô tả chi tiết những gì đã xảy ra và giúp người quản lý tìm cách để ngăn chặn một sự cố tương tự trong tương lai. Tùy thuộc vào quy mô của tổ chức và mức độ nghiêm trọng của sự việc, vị trí này có thể nhiều hơn một người.
- Chuyên viên quan hệ công chúng - Nếu cần thiết, thành viên này của đội phải nắm rõ tình hình và việc xử lý sự cố, sau đó anh ta làm việc như phát ngôn viên chính thức của tổ chức đến công chúng. Sau khi giải quyết một vấn đề, cả đội đánh giá lại những gì đã xảy ra, xác định cách vấn đề được ngăn chặn như thế nào, sau đó thực hiện các biện pháp để tránh sự việc xảy ra trong tương lai. Chỉ riêng chính sách an ninh không thể bảo vệ chống lại sự xâm nhập.

## 2.7 Vấn đề an ninh hệ thống.

An ninh hệ thống có thể bị đe doạ từ rất nhiều góc độ và nguyên nhân khác nhau gọi chung là các lỗ hổng bảo mật. Đe doạ an ninh có thể xuất phát từ bên ngoài mạng nội bộ hoặc cũng có thể xuất phát từ ngay bên trong tổ chức. Do đó, việc đảm bảo an ninh an toàn cho mạng máy tính cần phải có nhiều giải pháp cụ thể khác nhau. Tuy nhiên, tổng quan nhất có ba giải pháp cơ bản sau:

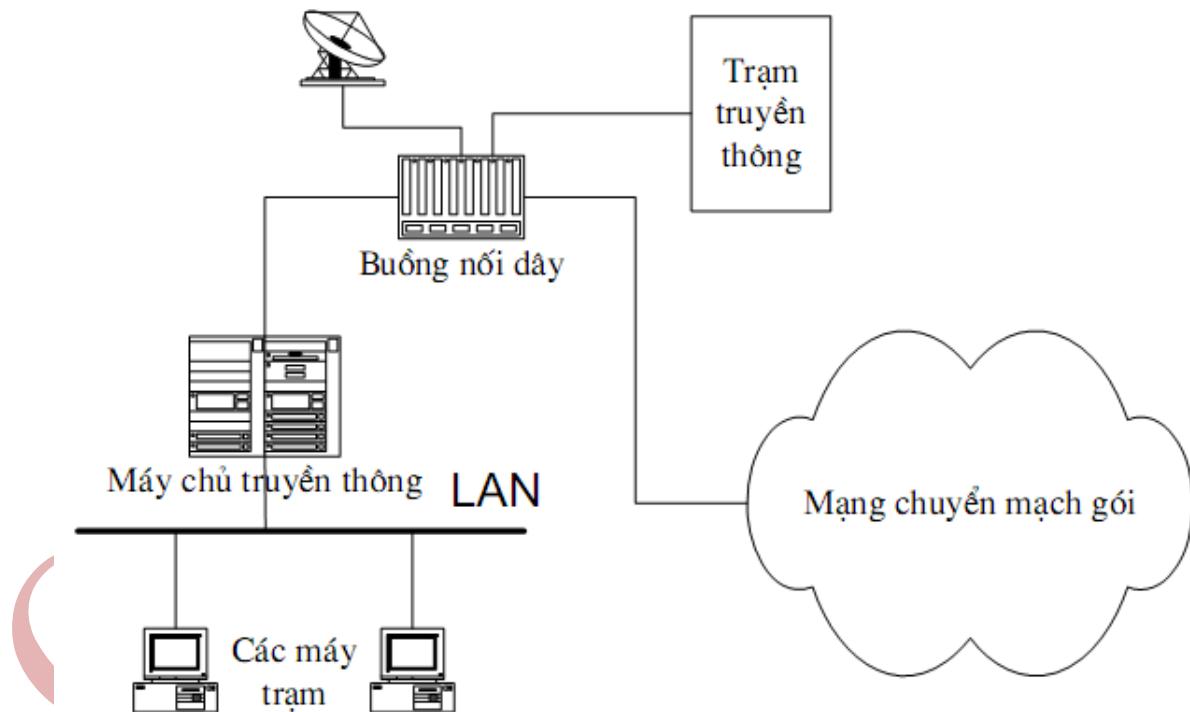
- Giải pháp về phần cứng.
- Giải pháp về phần mềm.
- Giải pháp về con người.

Đây là ba giải pháp tổng quát nhất mà bất kì một nhà quản trị an ninh nào cũng phải tính đến trong công tác đảm bảo an ninh an toàn mạng máy tính. Mỗi giải pháp có một ưu nhược

điểm riêng mà người quản trị an ninh cần phải biết phân tích, tổng hợp và chọn lựa để tạo khả năng đảm bảo an ninh tối ưu nhất cho tổ chức mình.

### Đảm bảo tính riêng tư.

Đối tượng tiềm tàng của tấn công riêng tư là các mạng quảng bá (LAN) và các điểm kết nối. Với phần lớn các mạng LAN là mạng quảng bá nên thông tin được truyền giữa hai máy có thể được các máy khác nhìn thấy. Thông tin truyền tải theo frame chứa địa chỉ nguồn và đích. Đối phương có thể quan sát sự chuyển tải trong LAN và xác định mọi traffic cần thiết dựa trên địa chỉ nguồn và đích. Nếu LAN cung cấp khả năng truy nhập theo đường dial-in, đối phương có thể truy cập vào mạng và theo dõi luồng truyền tải. Từ LAN truy cập ra ngoài thường thông qua: router, modem, server. Từ các comm server thường có các đường kết nối tới các patch panel. Với đối tượng là các điểm kết nối, đối phương có thể móc nối vào mạng thông qua các vị trí nối dây dùng các sóng điện từ năng lượng thấp để truyền tải thông tin ra ngoài.



Lưu ý: Các tấn công vào mạng có thể tại mọi vị trí của đường truyền thông. Đối với dạng tấn công chủ động, kẻ tấn công phải kiểm soát vật lý đường truyền và có thể thêm, bắt giữ thông tin.

### 2.7.1 Các cơ chế đảm bảo an toàn hệ thống.

- Cơ chế bảo mật đường liên kết

Mỗi đường truyền thông có thể bị tấn công đều được kết nối với các thiết bị mã hóa tại hai đầu ⇒ mọi quá trình truyền tải trên đường đều được bảo mật.

#### Nhược điểm:

- Yêu cầu nhiều thiết bị mã hóa
- Giải mã đối với mạng lớn.
- Thông điệp phải được giải mã mỗi khi đi vào bộ chuyển mạch gói bởi vì bộ chuyển mạch cần phải đọc địa chỉ ( virtual circuit number ) trong phần đầu gói tin để định tuyến cho gói.
- Như vậy thông điệp là một điểm yếu tại mỗi bộ chuyển mạch. Do đó nếu phải làm việc với mạng công cộng, người sử dụng không thể kiểm soát được an toàn thông tin tại nút mạng.

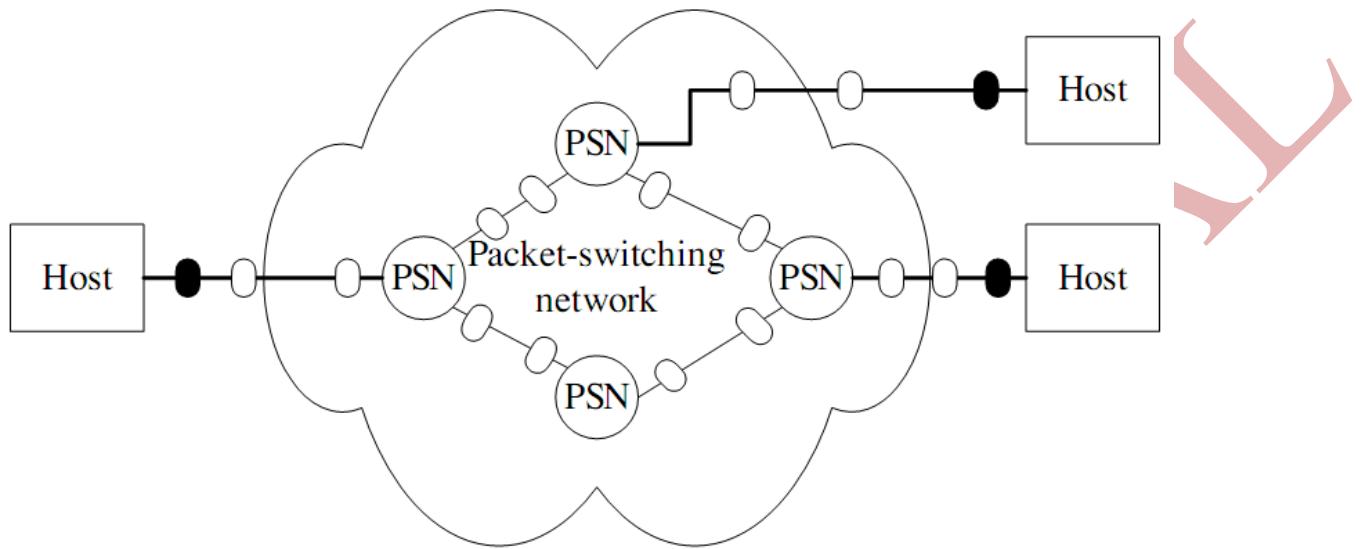
#### Biện pháp khắc phục:

- Mọi đường liên kết từ nguồn tin tới đích cần phải được đảm bảo mã mật.
- Mỗi cặp nút chia sẻ một đường kết nối phải cùng chia sẻ một khóa mật duy nhất và mỗi đường liên kết khác nhau phải dùng những khóa mật khác nhau.
- Như vậy phải dùng nhiều khóa và mỗi khóa chỉ được phân phối tới hai nút.

#### Cơ chế bảo mật đầu – cuối

Quá trình mã hóa mật được thực hiện tại hai hệ thống đầu cuối. Máy trạm nguồn mã hóa thông tin và được truyền qua mạng tới trạm đích. Trong đó, trạm nguồn và trạm đích cùng chia sẻ khóa mật và do đó có thể giải mã thông điệp. Dạng bảo mật này cho phép bảo

đảm an toàn đối với các tấn công vào các điểm kết nối hoặc các điểm chuyển mạch. Dạng bảo mật này cũng cho phép người sử dụng yên tâm về mức độ an toàn của mạng và đường liên kết truyền thông.



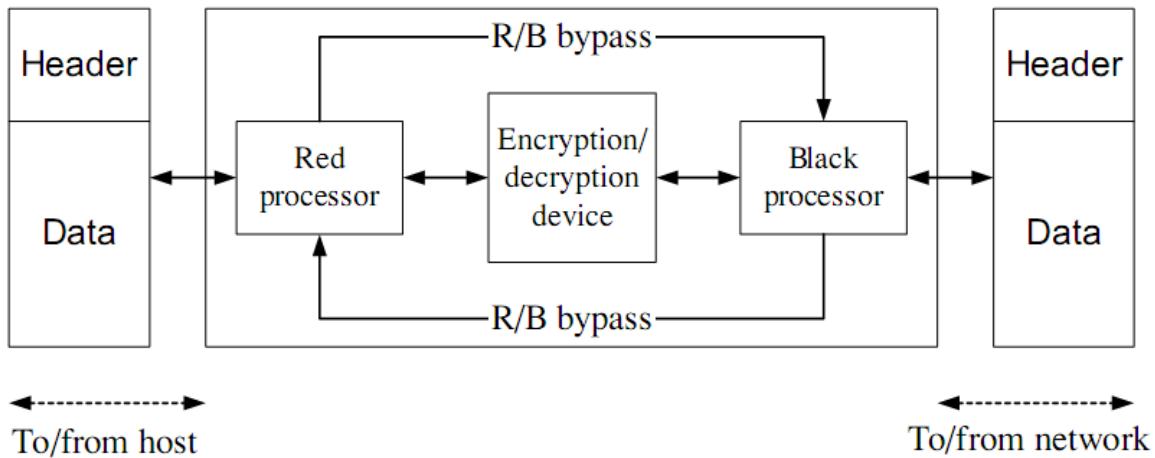
**Nhược điểm:** Dữ liệu truyền bao gồm phần đầu và phần dữ liệu: Nếu mã hóa toàn bộ gói tin theo sơ đồ mã hóa đối xứng, thông tin không thể truyền tới đích vì: chỉ có máy đích giải mã được gói tin  $\Rightarrow$  nút chuyển mạch không thể giải mã và đọc địa chỉ đích do đó không thể định tuyến gói tin. Bên cạnh đó, nếu chỉ mã hóa phần thân gói tin  $\Rightarrow$  đối phương sẽ biết phần đầu để phân tích tải.

**Ưu điểm:** Phương pháp bảo mật đầu cuối cho phép thực hiện xác thực: hai trạm đầu cuối chia sẻ cùng một khóa mật, người nhận sẽ biết được thông điệp tới từ người gửi. Phương pháp bảo mật đường truyền không có cơ chế xác thực.

### 2.7.2 Điểm đặt các hàm mã hóa đầu cuối.

Với mã hóa đường truyền, các hàm mã hóa được thực hiện tại mức thấp của phân cấp mạng truyền thông (tầng vật lý hoặc tầng liên kết). Đối với mã hóa đầu cuối, mức thấp nhất để đặt các hàm mã hóa là tầng mạng. Ví dụ: các phép mã hóa có thể được đặt tương ứng với X.25, do đó mọi khôi dữ liệu của các khôi X.25 đều được mã hóa. Trên mức mã hóa tầng mạng, số lượng các đối tượng được định danh và bảo vệ riêng rẽ tương ứng với số lượng trạm đầu cuối. Mỗi trạm đầu cuối có thể trao đổi mật mã với trạm khác nếu chúng

cùng chia sẻ một khóa mật. Như vậy có thể tách chức năng mã hóa và đưa vào một khối chức năng bộ xử lý ngoại vi.



### 2.7.3 Đảm bảo tính riêng tư cho luồng truyền tải.

Các thông tin có thể được biết bằng phân tích luồng truyền tải bao gồm:

- Định danh của các bên tham gia vào quá trình truyền tin.
- Tần suất truyền tải thông tin giữa hai bên tham gia.
- Mẫu thông điệp, độ dài thông điệp, số lượng thông điệp dùng để truyền tải những thông tin quan trọng.

Các sự kiện liên quan tới các đối thoại đặc biệt giữa hai bên tham gia trao đổi thông tin.

Một vấn đề liên quan tới luồng truyền tải là: có thể sử dụng mẫu của luồng để tạo các kênh vụng trộm.

Tùy vào cơ chế đảm bảo an toàn hệ thống ứng dụng mà có phương pháp thích hợp tương ứng là phương pháp mã mật đường liên kết và phương pháp bảo mật đầu cuối.

## 2.8 Trao đổi khóa và ứng dụng an toàn trên Internet

Trên môi trường mạng thực tế hiện nay, để đảm bảo các giao dịch trực tuyến như chuyển tiền online, mua hàng qua các trang web như eBay, Amazon, Google Play book... người ta thường sử dụng những giao thức đặc biệt được thiết kế để đảm bảo môi trường truyền dẫn giữa người dùng và server được bảo mật bằng mã hóa một cách tối đa. Vấn đề

an toàn giao thức truyền tải là một nhiệm vụ trọng tâm khi thiết kế một mạng mà chúng ta cần bảo vệ quá trình truyền tải từ người dùng cuối tới server chống lại mọi kiểu tấn công.

CONFIDENTIAL

## Chương 3: GIAO THỨC VÀ ỨNG DỤNG AN TOÀN

### 3.1 SSL

SSL (Secure Socket Layer) là giao thức đa mục đích được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước (socket 443) nhằm mã hoá toàn bộ thông tin đi/đến, mà ngày nay được sử dụng rộng rãi cho giao dịch điện tử như truyền số hiệu thẻ tín dụng, mật khẩu, số bí mật cá nhân (PIN) trên Internet.

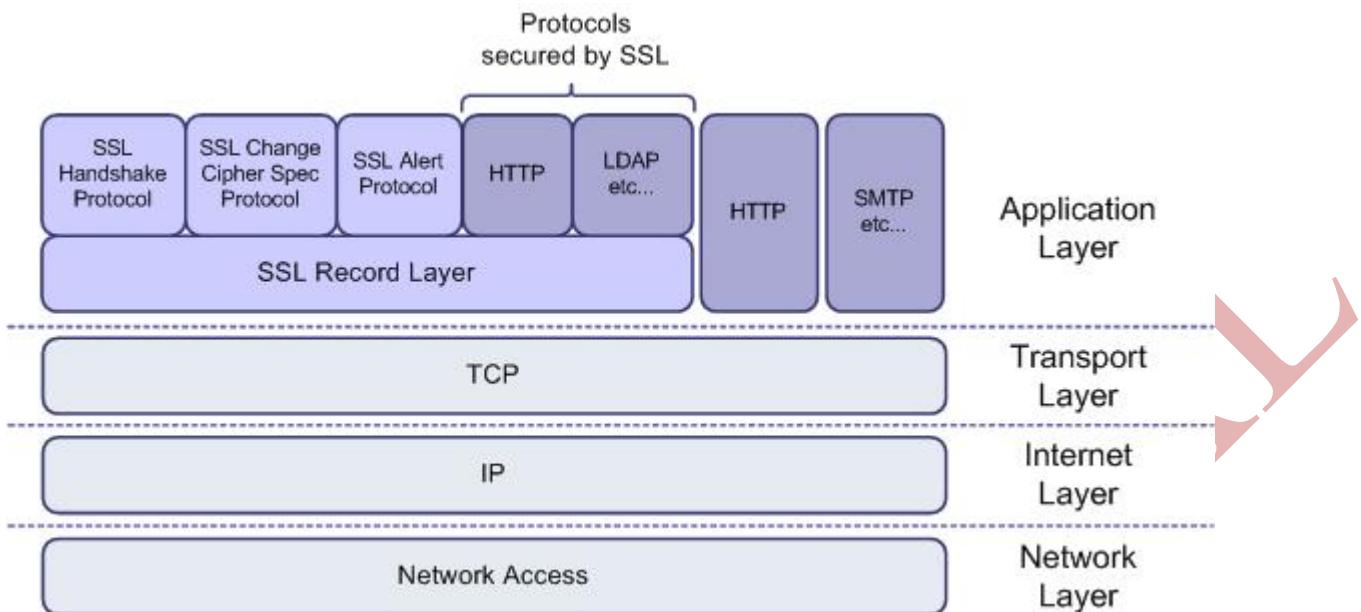
Giao thức SSL (Secure Socket Layer) tổ hợp nhiều giải thuật mã hóa nhằm đảm bảo quá trình trao đổi thông tin trên mạng được bảo mật. Việc mã hóa dữ liệu diễn ra một cách trong suốt, hỗ trợ nhiều giao thức khác chạy trên nền giao thức TCP. Sercure Socket Layer (SSL) hiện nay là giao thức bảo mật rất phổ biến trên Internet trong các hoạt động thương mại điện tử (E-Commerce).

Giao thức SSL được hình thành và phát triển đầu tiên năm 1994 bởi nhóm nghiên cứu Netscape dẫn dắt bởi Elgammal và ngày nay đã trở thành chuẩn bảo mật thực hành trên mạng Internet. Phiên bản SSL hiện nay là 3.0 và vẫn đang tiếp tục được bổ sung và hoàn thiện.

SSL là giao thức tầng (layered protocol), bao gồm 4 giao thức con sau:

- Giao thức SSL Handshake
- Giao thức SSL Change Cipher Spec
- Giao thức SSL Alert
- SSL Record Layer

Vị trí của các giao thức trên, tương ứng với mô hình TCP/IP được minh họa theo biểu đồ sau:



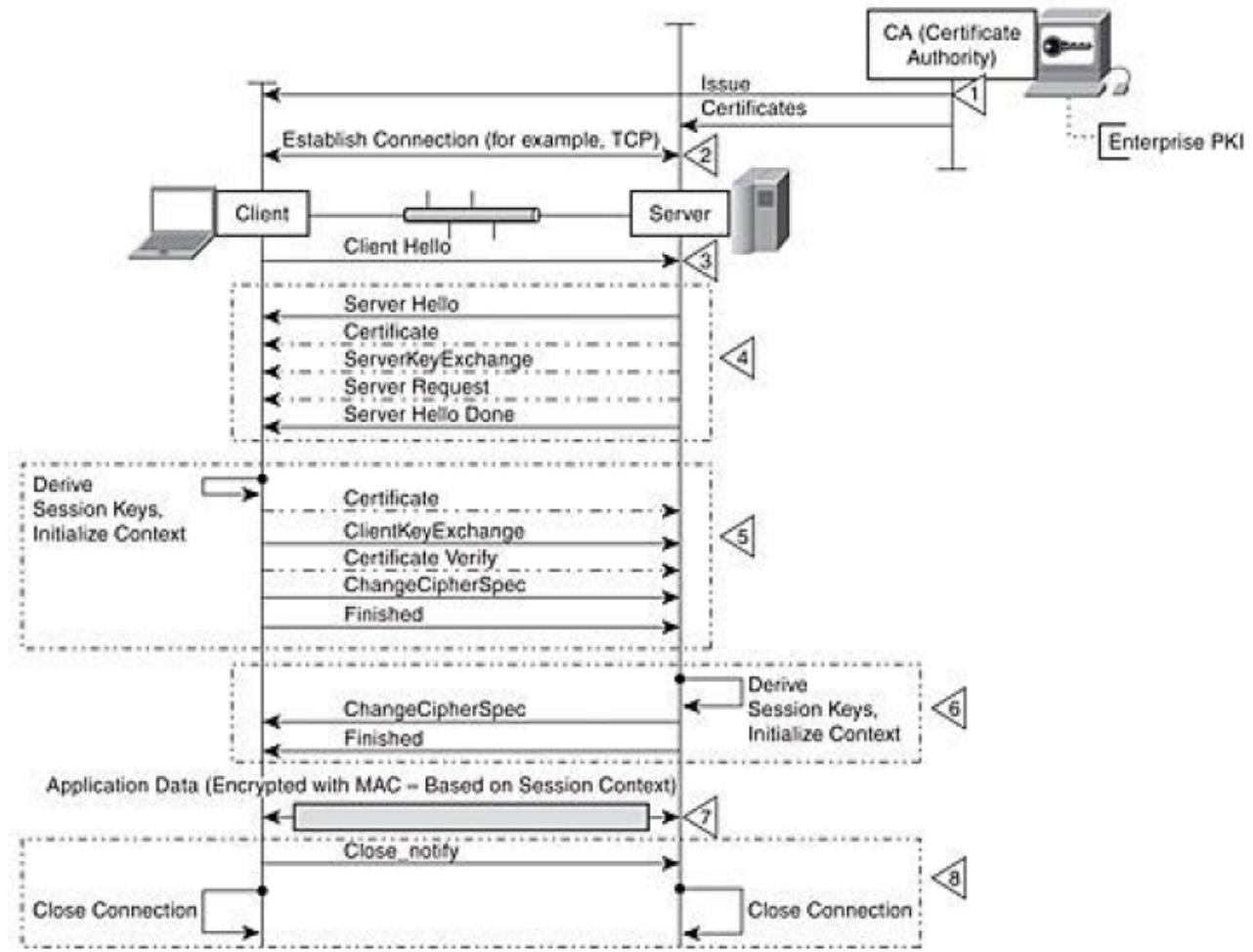
Theo biểu đồ trên, SSL nằm trong tầng ứng dụng của giao thức TCP/IP. Do đặc điểm này, SSL có thể được dùng trong hầu hết mọi hệ điều hành hỗ trợ TCP/IP mà không cần phải chỉnh sửa nhân của hệ thống hoặc ngăn xếp TCP/IP. Điều này mang lại cho SSL sự cải tiến mạnh mẽ so với các giao thức khác như IPSec (IP Security Protocol). Vì giao thức này đòi hỏi nhân hệ điều hành phải hỗ trợ và chỉnh sửa ngăn xếp TCP/IP. SSL cũng có thể dễ dàng vượt qua tường lửa và proxy, cũng như NAT (Network Address Translation) mà không cần nguồn cung cấp.

## Hoạt Động Của Giao Thức SSL

Điểm cơ bản của SSL được thiết kế độc lập với tầng ứng dụng để đảm bảo tính bí mật, an toàn và chống giả mạo luồng thông tin qua Internet giữa hai ứng dụng bất kỳ, thí dụ như webserver và các trình duyệt khách (browsers), do đó được sử dụng rộng rãi trong nhiều ứng dụng khác nhau trên môi trường Internet.

Toàn bộ cơ chế hoạt động và hệ thống thuật toán mã hoá sử dụng trong SSL được phổ biến công khai, trừ khoá chia sẻ tạm thời (session key) được sinh ra tại thời điểm trao đổi giữa hai ứng dụng là tạo ngẫu nhiên và bí mật đối với người quan sát trên mạng máy tính. Ngoài ra, giao thức SSL còn đòi hỏi ứng dụng chủ phải được chứng thực bởi một đối tượng lớp thứ ba (CA) thông qua giấy chứng thực điện tử (digital certificate) dựa trên mật mã công khai (thí dụ RSA).

Sau đây ta xem xét một cách khái quát cơ chế hoạt động của SSL để phân tích cấp độ an toàn của nó và các khả năng áp dụng trong các ứng dụng nhạy cảm, đặc biệt là các ứng dụng về thương mại và thanh toán điện tử...



Giao thức SSL dựa trên hai nhóm con giao thức là giao thức “bắt tay” (handshake protocol) và giao thức “bản ghi” (record protocol). Giao thức bắt tay xác định các tham số giao dịch giữa hai đối tượng có nhu cầu trao đổi thông tin hoặc dữ liệu, còn giao thức bản ghi xác định khuôn dạng cho tiến hành mã hoá và truyền tin hai chiều giữa hai đối tượng đó. Khi hai ứng dụng máy tính, thí dụ giữa một trình duyệt web và máy chủ web, làm việc với nhau, máy chủ và máy khách sẽ trao đổi “lời chào” (hellos) dưới dạng các thông điệp cho nhau với xuất phát đầu tiên chủ động từ máy chủ, đồng thời xác định các chuẩn về thuật toán mã hoá và nén số liệu có thể được áp dụng giữa hai ứng dụng. Ngoài ra, các ứng dụng còn trao đổi “số nhận dạng/khoá theo phiên” (session ID, session key) duy nhất cho lần làm

việc đó. Sau đó ứng dụng khách (trình duyệt) yêu cầu có chứng thực điện tử (digital certificate) xác thực của ứng dụng chủ (web server).

Chứng thực điện tử thường được xác nhận rộng rãi bởi một cơ quan trung gian (là CA -Certificate Authority) như RSA Data Security hay VeriSign Inc., một dạng tổ chức độc lập, trung lập và có uy tín. Các tổ chức này cung cấp dịch vụ “xác nhận” số nhận dạng của một công ty và phát hành chứng chỉ duy nhất cho công ty đó như là bằng chứng nhận dạng (identity) cho các giao dịch trên mạng, ở đây là các máy chủ webserver. Sau khi kiểm tra chứng chỉ điện tử của máy chủ (sử dụng thuật toán mật mã công khai, như RSA tại trình máy trạm), ứng dụng máy trạm sử dụng các thông tin trong chứng chỉ điện tử để mã hóa thông điệp gửi lại máy chủ mà chỉ có máy chủ đó có thể giải mã. Trên cơ sở đó, hai ứng dụng trao đổi khoá chính (master key) - khoá bí mật hay khoá đối xứng - để làm cơ sở cho việc mã hóa luồng thông tin/dữ liệu qua lại giữa hai ứng dụng chủ khách. Toàn bộ cấp độ bảo mật và an toàn của thông tin/dữ liệu phụ thuộc vào một số tham số: (i) số nhận dạng theo phiên làm việc ngẫu nhiên; (ii) cấp độ bảo mật của các thuật toán bảo mật áp dụng cho SSL; và (iii) độ dài của khoá chính (key length) sử dụng cho lược đồ mã hóa thông tin.

Các thuật toán mã hóa và xác thực của SSL được sử dụng bao gồm:

- DES (Data Encryption Standard) là một thuật toán mã hóa có chiều dài khoá là 56 bit.
- 3-DES (Triple-DES): là thuật toán mã hóa có độ dài khoá gấp 3 lần độ dài khoá trong mã hóa DES
- DSA (Digital Signature Algorithm): là một phần trong chuẩn về xác thực số đang được chính phủ Mỹ sử dụng.
- KEA (Key Exchange Algorithm) là một thuật toán trao đổi khoá đang được chính phủ Mỹ sử dụng.
- MD5 (Message Digest algorithm) được phát triển bởi Rivest.
- RSA: là thuật toán mã hóa công khai dùng cho cả quá trình xác thực và mã hóa dữ liệu được Rivest, Shamir, and Adleman phát triển.
- RSA key exchange: là thuật toán trao đổi khoá dùng trong SSL dựa trên thuật toán RSA.

- RC2 and RC4: là các thuật toán mã hoá được phát triển bởi Rivest dùng cho RSA Data Security.
- SHA-1 (Secure Hash Algorithm): là một thuật toán băm đang được chính phủ Mỹ sử dụng.

Khi một client và server trao đổi thông tin trong giai đoạn bắt tay (handshake), họ sẽ xác định bộ mã hoá mạnh nhất có thể và sử dụng chúng trong phiên giao dịch SSL

### 3.2 TLS

TLS (tiếng Anh: Transport Layer Security: "Bảo mật tầng truyền tải"), cùng với SSL (Secure Sockets Layer: "Tầng ô bảo mật") dẫn trước, là các giao thức mật mã nhằm mục đích bảo mật sự vận chuyển trên Internet. Các giao thức này mật mã hóa khóa bất đối xứng bằng các chứng thực X.509 để xác thực bên kia và để trao đổi một khóa đối xứng. Sau đó, khóa phiên được dùng để mã hóa các dữ liệu được truyền qua lại hai bên. Phương pháp này cho phép bảo mật dữ liệu hoặc thông điệp và xác thực tính toàn vẹn của các thông điệp qua các mã xác thực thông điệp (message authentication code). Vài biến thể được sử dụng rộng rãi trong các ứng dụng như duyệt Web, thư điện tử, fax qua Internet, nhắn tin nhanh, và VoIP. Một chính sách quan trọng, bí mật chuyển tiếp (forward secrecy), làm cho không thể tính ra khóa phiên ngắn hạn từ khóa bí mật bất đối xứng dài hạn.

Do sử dụng các chứng thực X.509, giao thức này cần các nhà cung cấp chứng thực số và hạ tầng khóa công khai để xác nhận mối quan hệ giữa một chứng thực và chủ của nó, cũng như để tạo, ký, và quản lý sự hiện lực của các chứng thực. Tuy quá trình này có thể tốt hơn việc xác nhận các danh tính qua một mạng lưới tín nhiệm, nhưng vụ tai tiếng do thám bí mật người dân 2013 đã báo động công cộng rằng các nhà cung cấp chứng thực là một điểm yếu về bảo mật vì cho phép các tấn công xen giữa (man-in-the-middle attack).

Trong khung nhìn mô hình TCP/IP, TLS và SSL đều mã hóa dữ liệu của các kết nối mạng trên một tầng phụ thấp của tầng ứng dụng. Theo hệ thống tầng cấp của mô hình OSI, TLS/SSL được khởi chạy ở tầng 5 (tầng phiên) rồi hoạt động trên tầng 6 (tầng trình diễn): trước tiên tầng phiên bắt tay dùng mật mã bất đối xứng để đặt cấu hình mật mã và chìa khóa chia sẻ dành cho phiên đó; sau đó, tầng trình diễn mã hóa phần còn lại của thông điệp dùng

mật mã đối xứng và khóa của phiên đó. Trong cả hai mô hình, TLS và SSL phục vụ tầng giao vận bên dưới, các đoạn trong tầng này chứa dữ liệu mật mã hóa.

Giao thức TLS trực thuộc chương trình tiêu chuẩn của IETF. Nó được định rõ lần đầu tiên năm 1999 và cập nhật lần cuối cùng trong RFC 5246 (tháng 8 năm 2008) và RFC 6176 (tháng 3 năm 2011). TLS phỏng theo các bản định rõ SSL về trước (1994, 1995, 1996) do Netscape Communications phát triển[5] nhằm thực hiện giao thức HTTPS trong trình duyệt Navigator.

### 3.3 HTTPS

HTTPS viết tắt của Hypertext Transfer Protocol Secure – Giao thức truyền siêu văn bản được mã hóa là một giao thức mạng được sử dụng phổ biến để đảm bảo quá trình truyền thông an toàn thông qua mạng Internet. HTTPS được phát triển dựa trên nền tảng giao thức HTTP nhưng được thêm thành phần bảo mật SSL/TLS ( Socket Secure Layer/Transport Layer Security) do đó nó mang các đặc tính bảo mật của SSL/TLS vào một phiên làm việc HTTP tiêu chuẩn.

Netscape Communications tạo ra HTTPS vào năm 1994 cho trình duyệt web Netscape Navigator. Ban đầu, HTTPS đã được sử dụng với SSL mã hóa. Phiên bản hiện hành của HTTPS được chính thức chỉ định bởi RFC 2818 Tháng 5 năm 2000.

HTTPS là mô hình URI trong đó có cú pháp giống như các mô hình tiêu chuẩn HTTP . Tuy nhiên , với kiểu tín hiệu HTTPS, trình duyệt sẽ sử dụng một lớp mã hóa gia tăng của SSL / TLS để bảo vệ giao thông . SSL đặc biệt phù hợp cho HTTP vì nó có thể cung cấp một số bảo vệ ngay cả khi chỉ có một bên của truyền thông được xác thực . Đây là trường hợp với các giao dịch HTTP trên Internet, nơi mà thường chỉ có máy chủ được xác thực.

HTTPS tạo ra một kênh an toàn trên một mạng không an toàn . Điều này đảm bảo bảo vệ hợp lý từ những kẻ nghe trộm và các cuộc tấn công kiểu chặn bắt thông tin , với điều kiện là bộ mã hoá đầy đủ được sử dụng và chứng chỉ máy chủ được xác minh và đáng tin cậy .

Giao thức HTTPS sử dụng port 443, giúp đảm bảo các tính chất sau của thông tin:

- **Tính tin cậy:** sử dụng phương thức encryption để đảm bảo rằng các thông điệp được trao đổi giữa client và server không bị kẻ thứ ba đọc được.
- **Tính toàn vẹn:** sử dụng phương thức hashing để cả client và server đều có thể tin tưởng rằng thông điệp mà chúng nhận được có không bị mất mát hay chỉnh sửa.
- **Tính xác thực:** sử dụng digital certificate để giúp client có thể tin tưởng rằng server/website mà họ đang truy cập thực sự là server/website mà họ mong muốn vào, chứ không phải bị giả mạo.

Sự an toàn của HTTPS là dựa trên đặc tính của TLS, trong đó sử dụng khóa công khai và bí mật dài hạn để trao đổi khóa phiên ngắn hạn và mã hóa luồng dữ liệu giữa máy khách và máy chủ.

Để đảm bảo một là nói chuyện với các đối tác ai muốn nói chuyện với , chứng chỉ số CA được sử dụng. Kết quả là , chúng cần có các cơ quan chứng nhận và cơ sở hạ tầng khóa công khai để xác minh mối quan hệ giữa chủ sở hữu của một chứng chỉ , giấy chứng nhận , cũng như để tạo ra , đăng ký , quản lý và tính hợp lệ của giấy chứng nhận. Thông thường có một số nhà cung cấp chứng thư bảo mật HTTPS nổi tiếng như VeriSign, GlobalSign, Comodo, Thawte....Nhà cung cấp sẽ đảm bảo các quá trình xác thực, xác minh chủ sở hữu website hoặc nội dung trong đó cũng như đảm bảo rằng, toàn bộ những nội dung trên website là đã được chứng thực. Thực tế là người dùng chỉ nên tin cậy nếu những điều kiện sau đây được thỏa mãn :

Trình duyệt hỗ trợ HTTPS và các giao thức SSL/TLS. Được cung cấp bởi những nhà cung cấp chứng thực hợp pháp và có nền tảng hệ thống tốt. Trang web được chứng nhận hợp lệ và được ký xác nhận bởi một nhà cung cấp chứng thực như Trusted Sign Giấy phép chứng nhận với thông tin rõ ràng về chủ thể của website như tên công ty hay địa chỉ công ty.

Ví dụ: Đây là một website được chứng thực bằng giao thức HTTPS và được cung cấp bởi VeriSign.



Nếu thông tin là không tin cậy, một cảnh báo sẽ được trình duyệt sử dụng



## Secure Connection Failed

svn.boost.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec\_error\_unknown\_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)

Trong việc triển khai phổ biến của HTTPS trên internet, HTTPS cung cấp xác thực của trang web và máy chủ web liên quan do đó giúp chống lại các cuộc tấn công dạng man-in-the-middle và đặc biệt quan trọng nếu nền tảng mạng đó là mạng Wifi công cộng hoặc các mạng không được bảo vệ. Ngoài ra, nó cung cấp mã hóa hai chiều của thông tin liên lạc giữa máy khách và máy chủ, trong đó bảo vệ chống lại nghe trộm và giả mạo hoặc giả mạo các nội dung của thông tin liên lạc. Trong thực tế, điều này cung cấp một sự đảm bảo hợp lý rằng một là giao tiếp với các trang web trang web là chính xác, cũng như đảm bảo rằng nội dung của thông tin liên lạc giữa người sử dụng và trang web không thể đọc được hoặc giả mạo bởi bất kỳ bên thứ ba. Trong lịch sử, các kết nối HTTPS được sử dụng chủ yếu cho

các giao dịch thanh toán trên World Wide Web , e-mail và các giao dịch nhạy cảm trong hệ thống thông tin của công ty . Từ những năm 2010, HTTPS bắt đầu thấy sử dụng rộng rãi để bảo vệ trang tính xác thực trên tất cả các loại của các trang web , bảo mật tài khoản và giữ thông tin liên lạc của người dùng, danh tính và trình duyệt web riêng tư .

### 3.4 SSH

SSH (Secure Shell) là một giao thức mạng dùng để thiết lập kết nối mạng một cách bảo mật. SSH hoạt động ở lớp trên trong mô hình phân lớp TCP/IP. Các công cụ SSH (như là OpenSSH,...) cung cấp cho người dùng cách thức để thiết lập kết nối mạng được mã hoá để tạo một kênh kết nối riêng tư. Hơn nữa tính năng tunneling của các công cụ này cho phép chuyển tải các giao vận theo các giao thức khác. Do vậy có thể thấy khi xây dựng một hệ thống mạng dựa trên SSH, chúng ta sẽ có một hệ thống mạng riêng ảo VPN đơn giản.

SSH là một chương trình tương tác giữa máy chủ và máy khách có sử dụng cơ chế mã hoá đủ mạnh nhằm ngăn chặn các hiện tượng nghe trộm, đánh cắp thông tin trên đường truyền. Các chương trình trước đây: telnet, rlogin không sử dụng phương pháp mã hoá. Vì thế bất cứ ai cũng có thể nghe trộm thậm chí đọc được toàn bộ nội dung của phiên làm việc bằng cách sử dụng một số công cụ đơn giản. Sử dụng SSH là biện pháp hữu hiệu bảo mật dữ liệu trên đường truyền từ hệ thống này đến hệ thống khác.

The screenshot shows a PuTTY terminal window titled "1andihelp.com - PuTTY". The session is using the username "u12345678". The password is entered and the user is prompted for it. The terminal then displays the standard Debian GNU/Linux welcome message, which states that the programs included are free software and that the distribution terms for each program are described in the individual files in /usr/share/doc/\*/\*copyright. It also states that Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY. The prompt "(uiserver):u12345678:~ >" is shown at the bottom, followed by a green cursor.

## Cách thức làm việc của SSH

SSH làm việc thông qua 3 bước đơn giản:

- Định danh host - xác định định danh của hệ thống tham gia phiên làm việc SSH.
- Mã hoá - thiết lập kênh làm việc mã hoá.
- Chứng thực - xác thực người sử dụng có quyền đăng nhập hệ thống.

### Định danh host

Việc định danh host được thực hiện qua việc trao đổi khoá. Mỗi máy tính có hỗ trợ kiểu truyền thông SSH có một khoá định danh duy nhất. Khoá này gồm hai thành phần: khoá riêng và khoá công cộng. Khoá công cộng được sử dụng khi cần trao đổi giữa các máy chủ với nhau trong phiên làm việc SSH, dữ liệu sẽ được mã hoá bằng khoá công khai và chỉ có thể giải mã bằng khoá riêng. Khi có sự thay đổi về cấu hình trên máy chủ: thay đổi chương trình SSH, thay đổi cơ bản trong hệ điều hành, khoá định danh cũng sẽ thay đổi. Khi đó mọi người sử dụng SSH để đăng nhập vào máy chủ này đều được cảnh báo về sự thay đổi này. Khi hai hệ thống bắt đầu một phiên làm việc SSH, máy chủ sẽ gửi khoá công

công của nó cho máy khách. Máy khách sinh ra một khoá phiên ngẫu nhiên và mã hoá khoá này bằng khoá công cộng của máy chủ, sau đó gửi lại cho máy chủ. Máy chủ sẽ giải mã khoá phiên này bằng khoá riêng của mình và nhận được khoá phiên. Khoá phiên này sẽ là khoá sử dụng để trao đổi dữ liệu giữa hai máy. Quá trình này được xem như các bước nhận diện máy chủ và máy khách.

## Mã hoá

Sau khi hoàn tất việc thiết lập phiên làm việc bảo mật (trao đổi khoá, định danh), quá trình trao đổi dữ liệu diễn ra thông qua một bước trung gian đó là mã hoá/giải mã. Điều đó có nghĩa là dữ liệu gửi/nhận trên đường truyền đều được mã hoá và giải mã theo cơ chế đã thoả thuận trước giữa máy chủ và máy khách. Việc lựa chọn cơ chế mã hoá thường do máy khách quyết định. Các cơ chế mã hoá thường được chọn bao gồm: 3DES, IDEA, và Blowfish. Khi cơ chế mã hoá được lựa chọn, máy chủ và máy khách trao đổi khoá mã hoá cho nhau. Việc trao đổi này cũng được bảo mật dựa trên định danh bí mật của các máy. Kẻ tấn công khó có thể nghe trộm thông tin trao đổi trên đường truyền vì không biết được khoá mã hoá. Các thuật toán mã hoá khác nhau và các ưu, nhược điểm của từng loại:

- 3DES (cũng được biết như Triple-DES) -- phương pháp mã hoá mặc định cho SSH.
- IDEA—Nhanh hơn 3DES, nhưng chậm hơn Arcfour và Blowfish.
- Arcfour—Nhanh, nhưng các vấn đề bảo mật đã được phát hiện.
- Blowfish—Nhanh và bảo mật, nhưng các phương pháp mã hoá đang được cải tiến.

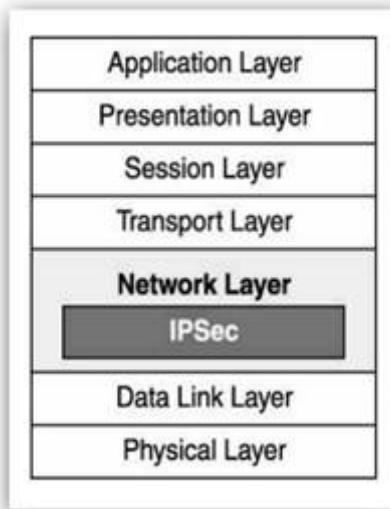
## Chứng thực

Việc chứng thực là bước cuối cùng trong ba bước, và là bước đa dạng nhất. Tại thời điểm này, kênh trao đổi bản thân nó đã được bảo mật. Mỗi định danh và truy nhập của người sử dụng có thể được cung cấp theo rất nhiều cách khác nhau. Chẳng hạn, kiểu chứng thực rhosts có thể được sử dụng, nhưng không phải là mặc định; nó đơn giản chỉ kiểm tra định danh của máy khách được liệt kê trong file rhost (theo DNS và địa chỉ IP). Việc chứng thực mật khẩu là một cách rất thông dụng để định danh người sử dụng, nhưng ngoài ra cũng

có các cách khác: chứng thực RSA, sử dụng ssh-keygen và ssh-agent để chứng thực các cặp khóa.

### 3.5 IPSec

IP Security (IPSec) là một giao thức được chuẩn hoá bởi IETF từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hoá và xác thực thông tin cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Hay nói cách khác, IPSec là sự tập hợp của các chuẩn mở được thiết lập để đảm bảo sự cần mật dữ liệu, đảm bảo tính toàn vẹn dữ liệu và chứng thực



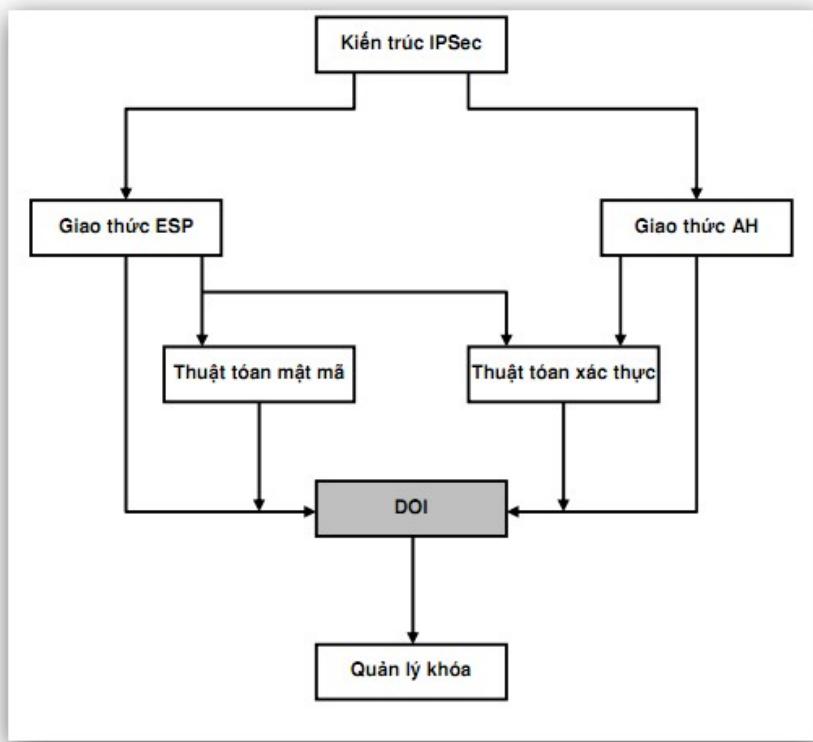
dữ liệu giữa các thiết bị mạng

IPSec cung cấp một cơ cấu bảo mật ở tầng 3 (Network layer) của mô hình OSI.

IPSec được thiết kế như phần mở rộng của giao thức IP, được thực hiện thống nhất trong cả hai phiên bản IPv4 và IPv6. Đối với IPv4, việc áp dụng IPSec là một tuỳ chọn, nhưng đối với IPv6, giao thức bảo mật này được triển khai bắt buộc.

#### Kiến trúc IPSec

IPSec là một giao thức phức tạp, dựa trên nền của nhiều kỹ thuật cơ sở khác nhau như mật mã, xác thực, trao đổi khoá... Xét về mặt kiến trúc, IPSec được xây dựng dựa trên các thành phần cơ bản sau đây, mỗi thành phần được định nghĩa trong một tài liệu riêng tương ứng:



- Kiến trúc IPsec (RFC 2401): Quy định các cấu trúc, các khái niệm và yêu cầu của IPsec.
- Giao thức ESP (RFC 2406): Mô tả giao thức ESP, là một giao thức mật mã và xác thực thông tin trong IPsec.
- Giao thức AH (RFC 2402): Định nghĩa một giao thức khác với chức năng gần giống ESP. Như vậy khi triển khai IPsec, người sử dụng có thể chọn dùng ESP hoặc AH, mỗi giao thức có ưu và nhược điểm riêng.
- Thuật toán mật mã: Định nghĩa các thuật toán mã hoá và giải mã sử dụng trong IPsec.
- IPsec chủ yếu dựa vào các thuật toán mã hoá đối xứng.
- Thuật toán xác thực: Định nghĩa các thuật toán xác thực thông tin sử dụng trong AH và ESP.
- Quản lý khoá (RFC 2408): Mô tả các cơ chế quản lý và trao đổi khoá trong IPsec.
- Miền thực thi (Domain of Interpretation – DOI): Định nghĩa môi trường thực thi IPsec.

IPSec không phải là một công nghệ riêng biệt mà là sự tổ hợp của nhiều cơ chế, giao thức và kỹ thuật khác nhau, trong đó mỗi giao thức, cơ chế đều có nhiều chế độ hoạt động khác nhau. Việc xác định một tập các chế độ cần thiết để triển khai IPSec trong một tình huống cụ thể là chức năng của miền thực thi. Xét về mặt ứng dụng, IPSec thực chất là một giao thức hoạt động song song với IP nhằm cung cấp 2 chức năng cơ bản mà IP nguyên thuỷ chưa có, đó là mã hoá và xác thực gói dữ liệu. Một cách khái quát có thể xem IPSec là một tổ hợp gồm hai thành phần:

- Giao thức đóng gói, gồm AH và ESP
- Giao thức trao đổi khoá IKE (Internet Key Exchange)

#### Các dịch vụ của IPSec:

- Quản lý truy xuất (access control)
- Toàn vẹn dữ liệu ở chế độ không kết nối (connectionless integrity)
- Xác thực nguồn gốc dữ liệu (data origin authentication )
- Chống phát lại (anti-replay)
- Mã hoá dữ liệu (encryption)
- Bảo mật dòng lưu lượng (traffic flow confidentiality)

Việc cung cấp các dịch vụ này trong từng tình huống cụ thể phụ thuộc vào giao thức đóng gói được dùng là AH hay ESP. Theo đó nếu giao thức được chọn là AH thì các dịch vụ mã hoá và bảo mật dòng dữ liệu sẽ không được cung cấp.

#### Ưu khuyết điểm của IPSec

##### a. Ưu điểm:

- Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng, thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan đến bảo mật.

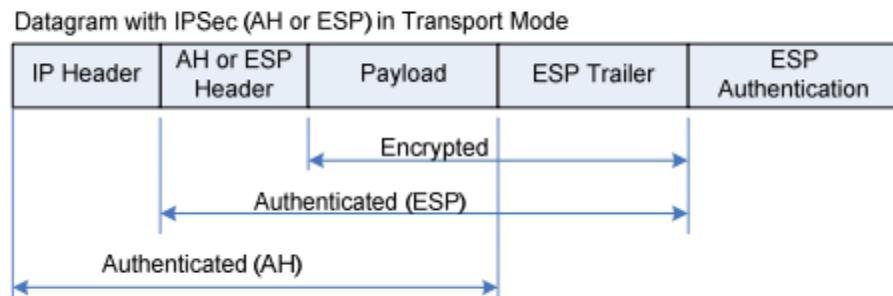
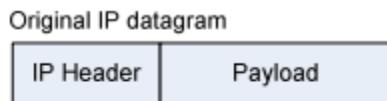
- IPSec được thực hiện bên dưới lớp TCP và UDP, đồng thời nó hoạt động trong suốt đối với các lớp này. Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
- IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối, điều này giúp che giấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua mạng Internet.

b. Hạn chế:

- Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kỹ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia

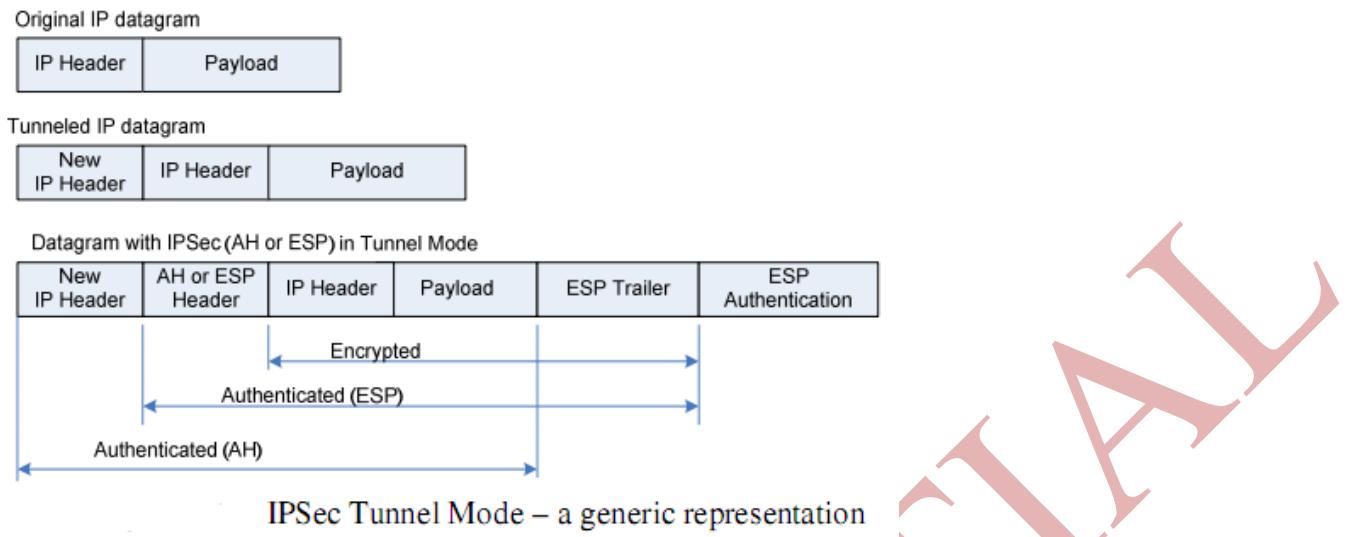
### Các chế độ hoạt động của IPSec:

- Transport Mode (chế độ vận chuyển): cung cấp cơ chế bảo vệ cho dữ liệu của các lớp cao hơn (TCP, UDP hoặc ICMP). Trong Transport mode, phần IPSec header được chèn vào giữa phần IP header và phần header của giao thức tầng trên, như hình mô tả bên dưới, AH và ESP sẽ được đặt sau IP header nguyên thủy. Vì vậy chỉ có tải (IP payload) là được mã hóa và IP header ban đầu là được giữ nguyên vẹn. Transport mode có thể được dùng khi cả hai host hỗ trợ IPSec. Chế độ transport này có thuận lợi là chỉ thêm vào vài bytes cho mỗi packets và nó cũng cho phép các thiết bị trên mạng thấy được địa chỉ đích cuối cùng của gói. Khả năng này cho phép các tác vụ xử lý đặc biệt trên các mạng trung gian dựa trên các thông tin trong IP header. Tuy nhiên các thông tin Layer 4 sẽ bị mã hóa, làm giới hạn khả năng kiểm tra của gói.



IPSec Transport-mode – a generic representation

- Tunnel mode : bảo vệ toàn bộ gói dữ liệu. Toàn bộ gói dữ liệu IP được đóng gói trong một gói dữ liệu IP khác và một IPSec header được chèn vào giữa phần đầu nguyên bản và phần đầu mới của IP. Toàn bộ gói IP ban đầu sẽ bị đóng gói bởi AH hoặc ESP và một IP header mới sẽ được bao bọc xung quanh gói dữ liệu. Toàn bộ các gói IP sẽ được mã hóa và trở thành dữ liệu mới của gói IP mới. Chế độ này cho phép những thiết bị mạng, chẳng hạn như router, hoạt động như một IPSec proxy thực hiện chức năng mã hóa thay cho host. Router nguồn sẽ mã hóa các packets và chuyển chúng dọc theo tunnel. Router đích sẽ giải mã gói IP ban đầu và chuyển nó về hệ thống cuối. Vì vậy header mới sẽ có địa chỉ nguồn chính là gateway. Với tunnel hoạt động giữa hai security gateway, địa chỉ nguồn và đích có thể được mã hóa. Tunnel mode được dùng khi một trong hai đầu của kết nối IPSec là security gateway và địa chỉ đích thật sự phía sau các gateway không có hỗ trợ IPSec



### 3.6 S/MIME

S/MIME là một chuẩn internet về định dạng cho mail. Hầu như mọi email trên internet đều được truyền qua giao thức SMTP theo định dạng MIME chưa có sự đảm bảo an toàn. Ví dụ, người gửi tin nhắn có thể dễ dàng giả mạo, tức là email nhận được mà không chắc có đúng là người mà mình mong muốn nhận tin hay tin nhắn có bị giả mạo hay không.Thêm vào đó, email thường không được mã hóa, có nghĩa rằng nếu một người nào đó truy cập vào hộp thư cá nhân thì có thể xem được email.

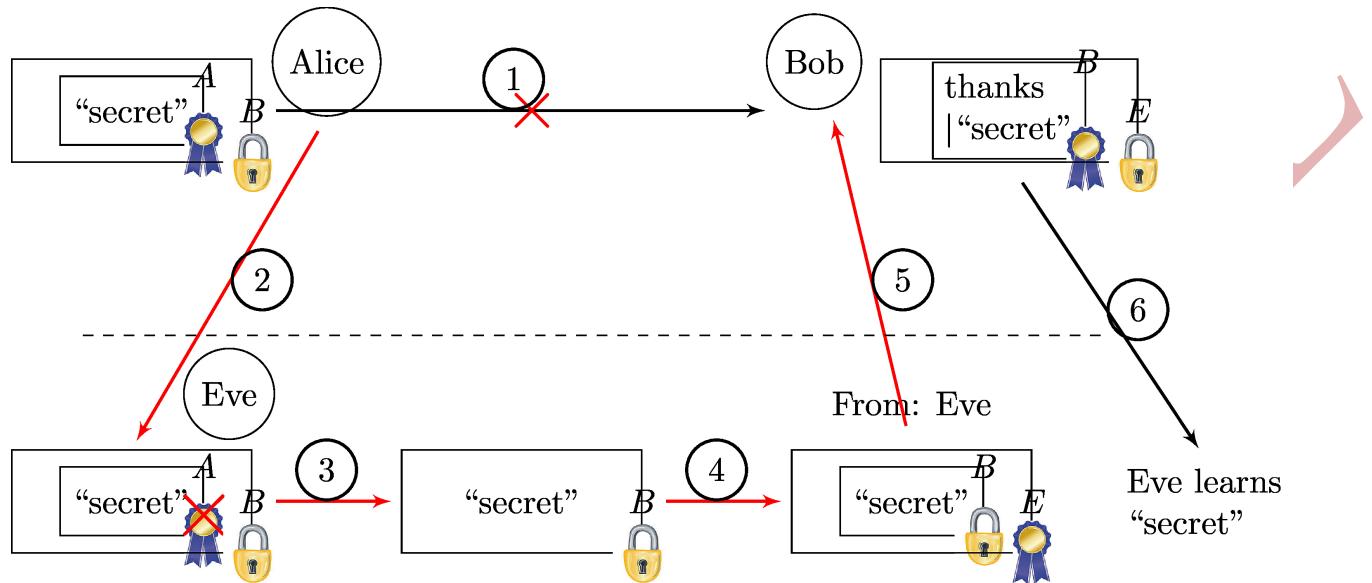
MIME khắc phục những hạn chế của SMTP (Simple Mail Transfer Protocol)

- ✓ Không truyền được file nhị phân (chương trình, ảnh,...)
- ✓ Chỉ gửi được các ký tự ASCII 7 bit
- ✓ Không nhận thông báo vượt quá kích thước cho phép

Giao thức S/MIME là một giải pháp an toàn thư điện tử. S/MIME đưa vào hai phương pháp an ninh cho email đó là mã hóa và chứng thực. Cả hai phương pháp đều dựa trên mã hóa bắt đối xứng và PKI.

S/MIME cung cấp một giải pháp cho quá trình gửi nhận dữ liệu 7 bit. S/mime có thể được sử dụng với những hệ thống cho phép truyền nhận dữ liệu MIME. Nó có thể được sử dụng cho các phương pháp gửi mail truyền thông có thêm dịch vụ an ninh cho mail gửi và

giải mã các dịch vụ an ninh cho bên nhận. S/MIME bảo vệ các thực thể MIME với chữ ký, mã hoặc cả hai. Để tạo ra một tin nhắn s/mime, Người dùng s/mime phải tuân theo các thông số kỹ thuật cũng như cú pháp của tin nhắn.



### 3.7 PGP

Mật mã hóa PGP® (Pretty Good Privacy®- Riêng tư tốt đẹp) là một phần mềm máy tính dùng để mật mã hóa dữ liệu và xác thực. Phiên bản PGP đầu tiên do Phil Zimmermann được công bố vào năm 1991. Kể từ đó, phần mềm này đã có nhiều cải tiến và hiện nay tập đoàn PGP cung cấp nhiều phần mềm dựa trên nền tảng này. Với mục tiêu ban đầu là phục vụ cho mã hóa thư điện tử, PGP hiện nay đã trở thành một giải pháp mã hóa cho các công ty lớn, chính phủ cũng như các cá nhân. Các phần mềm dựa trên PGP được dùng để mã hóa và bảo vệ thông tin lưu trữ trên máy tính xách tay, máy tính để bàn, máy chủ và trong quá trình trao đổi thông qua email, IM hoặc chuyển file. Giao thức hoạt động của hệ thống này có ảnh hưởng lớn và trở thành một trong hai tiêu chuẩn mã hóa (tiêu chuẩn còn lại là S/MIME).

### Ứng dụng của PGP

Mục tiêu ban đầu của PGP nhắm vào mật mã hóa nội dung các thông điệp thư điện tử và các tệp đính kèm cho người dùng phổ thông. Bắt đầu từ 2002, các sản phẩm PGP đã được đa dạng hóa thành một tập hợp ứng dụng mật mã và có thể được đặt dưới sự quản trị của một máy chủ. Các ứng dụng PGP giờ đây bao gồm: thư điện tử, chữ ký số, mật mã hóa

ở đĩa cứng máy tính xách tay, bảo mật tệp và thư mục, bảo mật các phiên trao đổi IM, mã hóa luồng chuyển tệp, bảo vệ các tệp và thư mục lưu trữ trên máy chủ mạng.

Phiên bản PGP Desktop 9.x dành cho máy để bàn bao gồm các tính năng: thư điện tử, chữ ký số, bảo mật IM, mã hóa ở đĩa cứng máy tính xách tay, bảo mật tệp và thư mục, tệp nén tự giải mã, xóa file an toàn. Các tính năng riêng biệt được cấp phép theo các cách khác nhau tùy theo yêu cầu.

Phiên bản PGP Universal 2.x dành cho máy chủ cho phép triển khai ứng dụng tập trung, thiết lập chính sách an ninh và lập báo cáo. Phần mềm này được dùng để mã hóa thư điện tử một cách tự động tại cổng ra vào (gateway) và quản lý các phần mềm máy khách PGP Desktop 9.x. Nó làm việc với máy chủ khóa công khai PGP (gọi là PGP Global Directory) để tìm kiếm khóa của người nhận và có khả năng gửi thư điện tử an toàn ngay cả khi không tìm thấy khóa của người nhận bằng cách sử dụng phiên làm việc HTTPS.

Với ứng dụng PGP Desktop 9.0 được quản lý bởi PGP Universal Server 2.0, tất cả các ứng dụng mã hóa PGP được dựa trên nền kiến trúc proxy mới. Các phần mềm này giúp loại bỏ việc sử dụng các plug-in của thư điện tử và tránh cho người dùng việc sử dụng các ứng dụng khác. Tất cả các hoạt động của máy chủ cũng như máy khách đều tự động tuân theo một chính sách an ninh. PGP Universal server còn tự động hóa các quá trình tạo, quản lý và kết thúc các khóa chia sẻ giữa các ứng dụng PGP.

Các phiên bản mới của PGP cho phép sử dụng cả 2 tiêu chuẩn: OpenPGP và S/MIME, cho phép trao đổi với bất kỳ ứng dụng nào tuân theo tiêu chuẩn của NIST.

## Hoạt động của PGP

PGP sử dụng kết hợp mã hóa khóa công khai và thuật toán khóa đối xứng cộng thêm với hệ thống xác lập mối quan hệ giữa khóa công khai và chỉ danh người dùng (ID). Phiên bản đầu tiên của hệ thống này thường được biết dưới tên mạng lưới tín nhiệm dựa trên các mối quan hệ ngang hàng (khác với hệ thống X.509 với cấu trúc cây dựa vào các nhà cung cấp chứng thực số). Các phiên bản PGP về sau dựa trên các kiến trúc tương tự như hạ tầng khóa công khai.

PGP sử dụng thuật toán mật mã hóa khóa bất đối xứng. Trong các hệ thống này, người sử dụng đầu tiên phải có một cặp khóa: khóa công khai và khóa bí mật. Người gửi sử dụng khóa công khai của người nhận để mã hóa một khóa chung (còn gọi là khóa phiên) dùng trong các thuật toán mật mã hóa khóa đối xứng. Khóa phiên này chính là khóa để mật mã hóa các thông tin được gửi qua lại trong phiên giao dịch. Rất nhiều khóa công khai của những người sử dụng PGP được lưu trữ trên các máy chủ khóa PGP trên khắp thế giới (các máy chủ mirror lẫn nhau).

Người nhận trong hệ thống PGP sử dụng khóa phiên để giải mã các gói tin. Khóa phiên này cũng được gửi kèm với thông điệp nhưng được mã hóa bằng hệ thống mật mã bất đối xứng và có thể tự giải mã với khóa bí mật của người nhận. Hệ thống phải sử dụng cả 2 dạng thuật toán để tận dụng ưu thế của cả hai: thuật toán bất đối xứng đơn giản việc phân phối khóa còn thuật toán đối xứng có ưu thế về tốc độ (nhanh hơn cỡ 1000 lần).

Một chiến lược tương tự cũng được dùng (mặc định) để phát hiện xem thông điệp có bị thay đổi hoặc giả mạo người gửi. Để thực hiện 2 mục tiêu trên người gửi phải ký văn bản với thuật toán RSA hoặc DSA. Đầu tiên, PGP tính giá trị hàm băm của văn bản đó rồi tạo ra chữ ký số với khóa bí mật của người gửi và gửi cả văn bản và chữ ký số đến người nhận. Khi nhận được văn bản, người nhận tính lại giá trị băm của văn bản đó đồng thời giải mã chữ ký số bằng khóa công khai của người gửi. Nếu 2 giá trị băm này giống nhau thì có thể khẳng định (với xác suất rất cao) là văn bản chưa bị thay đổi kể từ khi gửi và người gửi đúng là người sở hữu khóa bí mật tương ứng.

Trong quá trình mã hóa cũng như kiểm tra chữ ký, một điều vô cùng quan trọng là khóa công khai được sử dụng thực sự thuộc về người được cho là sở hữu nó. Nếu chỉ đơn giản là download một khóa công khai từ đâu đó sẽ không thể đảm bảo được điều này. PGP thực hiện việc phân phối khóa thông qua chứng thực số được tạo nên bởi những kỹ thuật mật mã sáo cho việc sửa đổi (không hợp pháp) có thể dễ dàng bị phát hiện. Tuy nhiên chỉ điều này thôi thì chưa đủ vì nó chỉ ngăn chặn được việc sửa đổi sau khi chứng thực đã được tạo ra. Người dùng còn cần phải được trang bị khả năng kiểm tra xem khóa công khai có

thực sự thuộc về người được cho là sở hữu hay không. Từ phiên bản đầu tiên, PGP đã có một cơ chế hỗ trợ điều này gọi là mạng lưới tín nhiệm. Mỗi khóa công khai (rộng hơn là các thông tin gắn với một khóa hay một người) đều có thể được một bên thứ 3 xác nhận (theo cách điện tử).

Trong các đặc tả gần đây của OpenPGP, các chữ ký tin cậy có thể được sử dụng để tạo ra các nhà cung cấp chứng thực số (CA). Một chữ ký tin cậy có thể chứng tỏ rằng một khóa thực sự thuộc về một người sử dụng và người đó đáng tin cậy để ký xác nhận một khóa của mức thấp hơn. Một chữ ký có mức 0 tương đương với chữ ký trong mô hình mạng lưới tín nhiệm. Chữ ký ở mức 1 tương đương với chữ ký của một CA vì nó có khả năng xác nhận cho một số lượng không hạn chế chữ ký ở mức 0. Chữ ký ở mức 2 tương tự như chữ ký trong danh sách các CA mặc định trong Internet Explorer; nó cho phép người chủ tạo ra các CA khác.

PGP cũng được thiết kế với khả năng hủy bỏ/thu hồi các chứng thực có khả năng đã bị vô hiệu hóa. Về một khía cạnh nào đó, điều này tương đương với danh sách chứng thực bị thu hồi của mô hình hạ tầng khóa công khai. Các phiên bản PGP gần đây cũng hỗ trợ tính năng hạn sử dụng của chứng thực.

Vấn đề xác định mối quan hệ giữa khóa công khai và người sở hữu không phải là vấn đề riêng của PGP. Tất cả các hệ thống sử dụng cặp khóa công khai và khóa bí mật đều phải đối phó với vấn đề này và cho đến nay chưa có một giải pháp hoàn thiện nào được tìm ra. Mô hình ban đầu của PGP trao cho quyền quyết định cuối cùng người sử dụng còn các mô hình PKI thì quy định tất cả các chứng thực phải được xác nhận (có thể không trực tiếp) bởi một nhà cung cấp chứng thực trung tâm.

## Chương 4: AN NINH HỆ THỐNG

### 4.1 Kỹ thuật phát hiện xâm nhập trái phép

Nếu như hiểu Firewall là một hệ thống “khóa” chốt chặn ở cửa ngõ mạng, thì hệ thống IDS có thể được coi như các “cảm ứng giám sát” được đặt khắp nơi trong mạng để cảnh báo về các cuộc tấn công đã “qua mặt” được Firewall hoặc xuất phát từ bên trong mạng. Một IDS có nhiệm vụ phân tích các gói tin mà Firewall cho phép đi qua, tìm kiếm các dấu hiệu tấn công từ các dấu hiệu đã biết hoặc thông qua việc phân tích các sự kiện bất thường, từ đó ngăn chặn các cuộc tấn công trước khi nó có thể gây ra những hậu quả xấu với tổ chức.

Hệ thống IDS hoạt động dựa trên 3 thành phần chính là Cảm ứng (Sensor), Giao diện (Console) và Bộ phân tích (Engine). Xét trên chức năng IDS có thể phân làm 2 loại chính là Network-based IDS (NIDS) và Host-based IDS (HIDS). NIDS thường được đặt tại cửa ngõ mạng để giám sát lưu thông trên một vùng mạng, còn HIDS thì được cài đặt trên từng máy trạm để phân tích các hành vi và dữ liệu đi đến máy trạm đó. Xét về cách thức hoạt động thì hệ thống IDS có thể chia làm 5 giai đoạn chính là: Giám sát, Phân tích, Liên lạc, Cảnh báo và Phản Ứng.

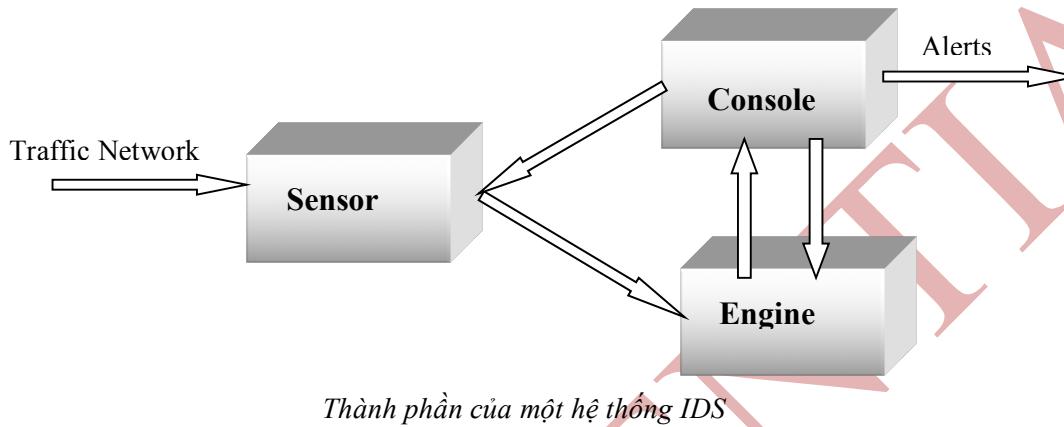
Thời gian gần đây, sự hoành hành của virus, worm nhầm vào hệ điều hành rất lớn. Nhiều loại virus, worm dùng phương pháp quét cổng theo địa chỉ để tìm ra lỗ hổng và sau đó mới lây lan vào. Với những loại tấn công này nếu hệ thống mạng có cài đặt hệ thống IDS thì khả năng phòng tránh được sẽ rất lớn.

#### 4.1.1. Thành phần

Một hệ thống IDS bao gồm 3 thành phần cơ bản là:

- ✓ **Cảm ứng (Sensor):** Là bộ phận làm nhiệm vụ phát hiện các sự kiện có khả năng đe dọa an ninh của hệ thống mạng, Sensor có chức năng rà quét nội dung của các gói tin trên mạng, so sánh nội dung với các mẫu và phát hiện ra các dấu hiệu tấn công hay còn gọi là sự kiện.

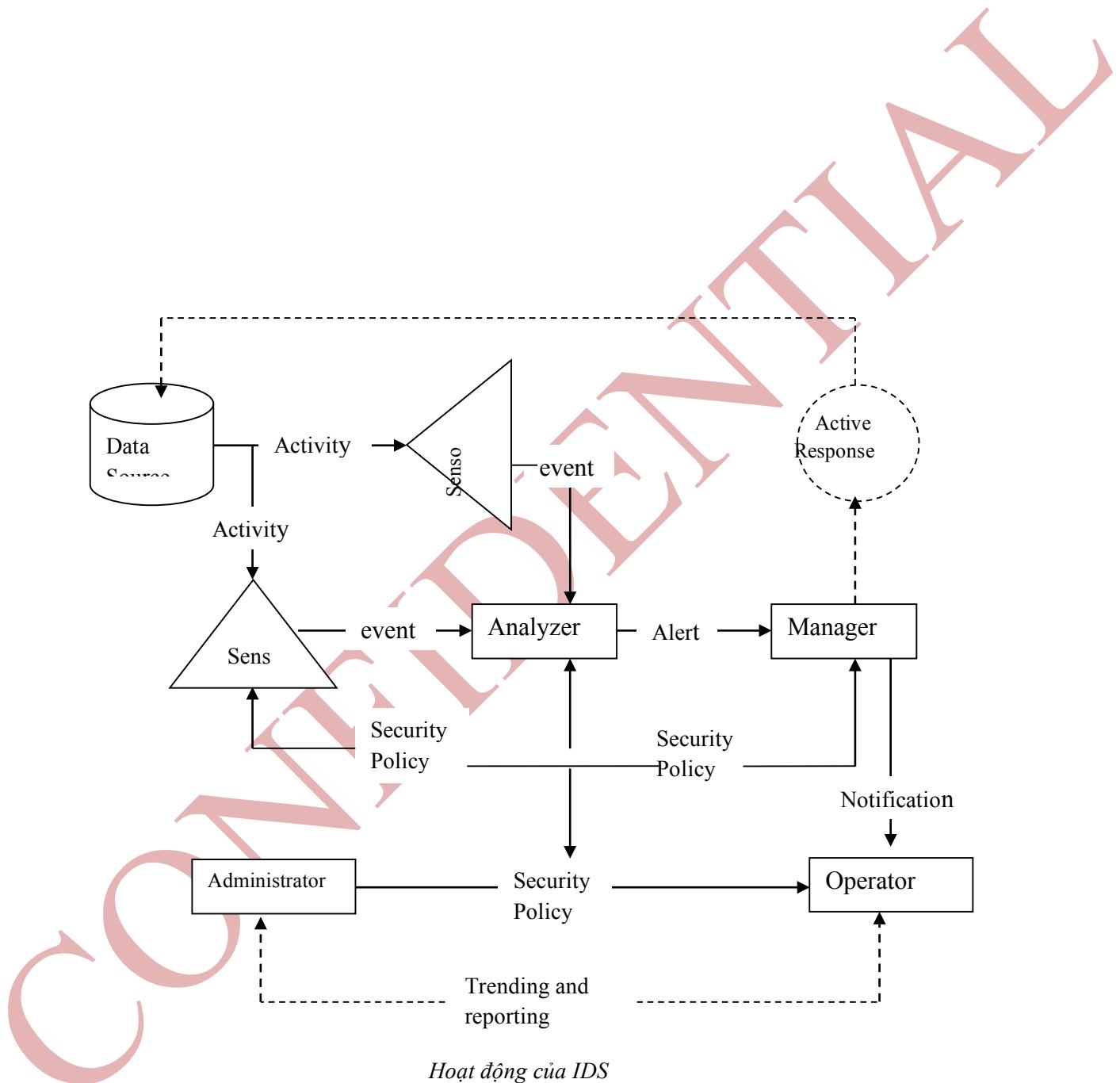
- ✓ **Giao diện (Console)**: Là bộ phận làm nhiệm vụ tương tác với người quản trị, nhận lệnh điều khiển hoạt động bộ Sensor, Engine và đưa ra cảnh báo tấn công.
- ✓ **Bộ xử lý (Engine)**: Có nhiệm vụ ghi lại tất cả các báo cáo về các sự kiện được phát hiện bởi các Sensor trong một cơ sở dữ liệu và sử dụng một hệ thống các luật để đưa ra các cảnh báo trên các sự kiện an ninh nhận được cho hệ thống hoặc cho người quản trị.



Như vậy, hệ thống IDS hoạt động theo cơ chế “phát hiện và cảnh báo”. Các Sensor là bộ phận được bố trí trên hệ thống tại những điểm cần kiểm soát, Sensor bắt các gói tin trên mạng, phân tích gói tin để tìm các dấu hiệu tấn công, nếu các gói tin có dấu hiệu tấn công, Sensor lập tức đánh dấu đây là một sự kiện và gửi báo cáo kết quả về cho Engine, Engine ghi nhận tất cả các báo cáo của tất cả các Sensor, lưu các báo cáo vào trong cơ sở dữ liệu của mình và quyết định đưa ra mức cảnh báo đối với sự kiện nhận được. Console làm nhiệm vụ giám sát, cảnh báo đồng thời điều khiển hoạt động của các Sensor.

Đối với các IDS truyền thống, các Sensor hoạt động theo cơ chế “so sánh mẫu”, các Sensor bắt các gói tin trên mạng, đọc nội dung gói tin và so sánh các xâu trong nội dung gói tin với hệ thống các mẫu tín hiệu nhận biết các cuộc tấn công hoặc mã độc gây hại cho hệ thống, nếu trong nội dung gói tin có một xâu trùng với mẫu, Sensor đánh dấu đó là một sự kiện hay đã có dấu hiệu tấn công và sinh ra cảnh báo. Các tín hiệu nhận biết các cuộc tấn công được tổng kết và tập hợp thành một bộ gọi là mẫu(signatures). Thông thường các mẫu

này được hình thành dựa trên kinh nghiệm phòng chống các cuộc tấn công, người ta thành lập các trung tâm chuyên nghiên cứu và đưa ra các mẫu này để cung cấp cho hệ thống IDS trên toàn thế giới.



## 4.1.2 Phân loại

Có nhiều cách để phân loại các hệ thống IDS tùy theo các tiêu chí khác nhau. Cách phân loại dựa trên hành vi của IDS có thể phân làm 2 loại là phát hiện xâm nhập dựa trên dấu hiệu (Misuse-based IDS) và phát hiện xâm nhập dựa trên dấu hiệu bất thường (Anomaly-based IDS – Xem chương 2):

Nếu xét về đối tượng giám sát thì có 2 loại IDS cơ bản nhất là: Host-based IDS và Network-based IDS. Từng loại có một cách tiếp cận khác nhau nhằm theo dõi và phát hiện xâm nhập, đồng thời cũng có những lợi thế và bất lợi riêng. Nói một cách ngắn gọn, Host-based IDS giám sát dữ liệu trên những máy tính riêng lẻ trong khi Network-based IDS giám sát lưu thông của một hệ thống mạng.

### 4.1.2.1 Host-based IDS (HIDS)

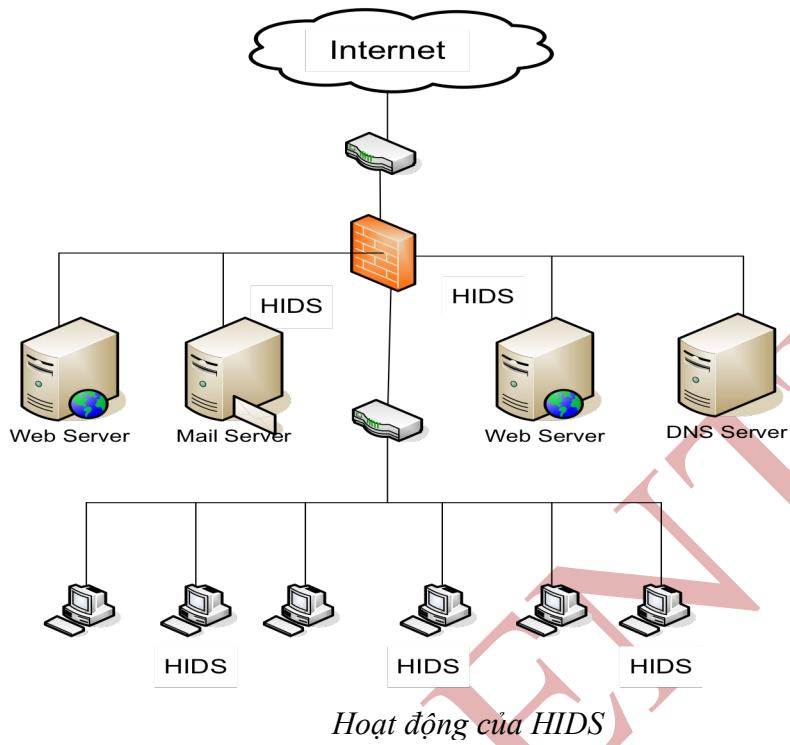
Những hệ thống Host-based là kiểu IDS được nghiên cứu và triển khai đầu tiên. Bằng cách cài đặt những phần mềm IDS trên các máy trạm (gọi là Agent), HIDS có thể giám sát toàn bộ hoạt động của hệ thống, các log file và lưu thông mạng đi tới từng máy trạm.

HIDS kiểm tra lưu thông mạng đang được chuyển đến máy trạm, bảo vệ máy trạm thông qua việc ngăn chặn các gói tin nghi ngờ. HIDS có khả năng kiểm tra hoạt động đăng nhập vào máy trạm, tìm kiếm các hoạt động không bình thường như dò tìm password, leo thang đặc quyền . . . Ngoài ra HIDS còn có thể giám sát sâu vào bên trong Hệ điều hành của máy trạm để kiểm tra tính toàn vẹn của Nhân hệ điều hành, file lưu trữ trong hệ thống . . .

Hệ thống IDS có hiệu quả cao khi phát hiện việc người dùng sử dụng sai các tài nguyên trên mạng. Nếu người dùng cố gắng thực hiện các hành vi không hợp pháp thì những hệ thống HIDS thông thường phát hiện và tập hợp thông tin thích hợp nhất và nhanh nhất.

Điểm yếu của HIDS là công kềnh. Với vài ngàn máy trạm trên một mạng lớn, việc thu thập và tập hợp các thông tin máy tính đặc biệt riêng biệt cho mỗi máy riêng lẻ là không

có hiệu quả. Ngoài ra, nếu thủ phạm vô hiệu hóa việc thu thập dữ liệu trên máy tính thì HIDS trên máy đó sẽ không còn có ý nghĩa.



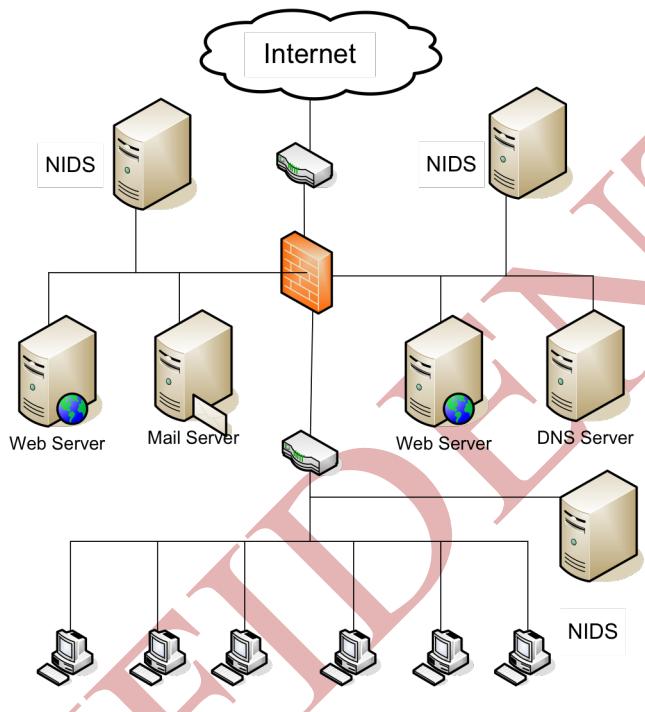
#### 4.1.2.2 Network-based IDS (NIDS)

NIDS là một giải pháp xác định các truy cập trái phép bằng cách kiểm tra các luồng thông tin trên mạng và giám sát nhiều máy trạm, NIDS truy nhập vào luồng thông tin trên mạng bằng cách kết nối vào các Hub, Switch để bắt các gói tin, phân tích nội dung gói tin và từ đó sinh ra các cảnh báo.

Trong hệ thống NIDS, các Sensor được đặt ở các điểm cần kiểm tra trong mạng, thường là trước miền DMZ() hoặc ở vùng biên của mạng, các Sensor bắt tất cả các gói tin lưu thông trên mạng và phân tích nội dung bên trong của từng gói để phát hiện các dấu hiệu tấn công trong mạng.

Điểm yếu của NIDS là gây ảnh hưởng đến băng thông do trực tiếp truy cập vào lưu thông mạng. NIDS không được định lượng đúng về khả năng xử lý sẽ trở thành một

nút cỗ chai gây ách tắc trong mạng. Ngoài ra NIDS còn gặp khó khăn với các vấn đề giao thức truyền như việc phân tách gói tin (IP fragmentation), hay việc điều chỉnh thông số TTL trong gói tin IP . . .



Hoạt động của NIDS

HIDS	NIDS
Tính quản trị thấp.	Quản trị tập trung.
Dễ cài đặt	Khó cài đặt
Tính bao quát thấp. Do mỗi máy trạm chỉ nhận được traffic của máy đó cho nên không thể có cái nhìn	Tính bao quát cao do có cái nhìn toàn diện về traffic mạng.

tổng hợp về cuộc tấn công.	
Phụ thuộc vào Hệ điều hành. Do HIDS được cài đặt trên máy trạm nên phụ thuộc vào Hệ điều hành trên máy đó.	Không phụ thuộc vào HDH của máy trạm.
Không ảnh hưởng đến băng thông mạng.	NIDS do phân tích trên luồng dữ liệu chính nên có ảnh hưởng đến băng thông mạng.
Không gặp vấn đề về giao thức	Gặp vấn đề về giao thức truyền: Packet Fragment, TTL.
	Vấn đề mã hóa: Nếu IDS được đặt trong một kênh mã hóa thì sẽ không phân tích được gói tin

IP fragmentation<sup>1</sup>: Là quá trình chia nhỏ gói tin khi thiết bị Switch hay Router phát hiện gói tin có kích thước to hơn khả năng xử lý của nó (kích thước gói tin gọi là MTU - Maximum transmission Unit).

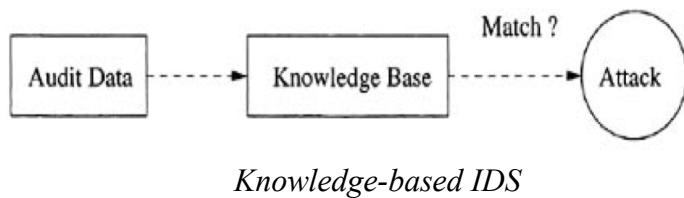
#### *Phân loại dựa trên dấu hiệu*

Misuse-based IDS có thể phân chia thành hai loại dựa trên cơ sở dữ liệu về kiểu tấn công đó là: Knowledge-based và Signature-based:

##### **4.1.2.3 Knowledge-based IDS**

Misuse-based IDS với cơ sở dữ liệu knowledge-based lưu trữ thông tin về các dạng tấn công. Dữ liệu kiểm kê được thu thập bởi IDS để so sánh với nội dung của cơ sở dữ liệu, và nếu thấy có sự giống nhau thì tạo ra cảnh báo. Sự kiện không giống với bất cứ dạng tấn công nào thì được coi là những hành động chính đáng. Lợi thế của mô hình này là chúng ít khi tạo ra cảnh báo sai do dựa trên mô tả chi tiết về kiểu tấn công. Tuy nhiên mô hình này có điểm yếu, trước tiên với số lượng kiểu tấn công đa dạng với nhiều lỗ hổng khác nhau theo thời gian sẽ làm cơ sở dữ liệu trở nên quá lớn, gây khó khăn trong việc phân tích, thêm

nữa chúng chỉ có thể phát hiện được các kiểu tấn công đã biết trước nên cần phải được cập nhật thường xuyên khi phát hiện ra những kiểu tấn công và lỗ hổng mới.



#### 4.1.2.4 Signature-based IDS

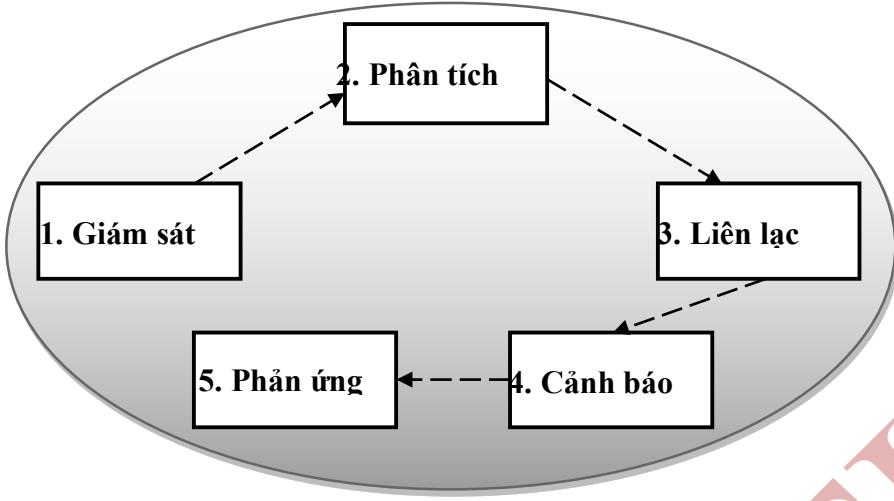
Signature-based IDS là hệ sử dụng định nghĩa trừu tượng để mô tả về tấn công gọi là dấu hiệu. Dấu hiệu bao gồm một nhóm các thông tin cần thiết để mô tả kiểu tấn công. Ví dụ như hệ network IDS có thể lưu trữ trong cơ sở dữ liệu nội dung các gói tin có liên quan đến kiểu tấn công đã biết. Thường thì dấu hiệu được lưu ở dạng cho phép so sánh trực tiếp với thông tin có trong chuỗi sự kiện. Trong quá trình xử lý, sự kiện được so sánh với các mục trong file dấu hiệu, nếu thấy có sự giống nhau thì hệ tạo ra cảnh báo. Signature-based IDS hiện nay rất thông dụng vì chúng dễ phát triển, cho phản hồi chính xác về cảnh báo và thường yêu cầu ít tài nguyên tính toán. Tuy nhiên, chúng có những điểm yếu sau:

- Mô tả về cuộc tấn công thường ở mức độ thấp, khó hiểu.
- Mỗi cuộc tấn công hay biến thể của nó đều cần thêm dấu hiệu đưa vào cơ sở dữ liệu, nên kích cỡ của nó sẽ trở nên rất lớn.
- Dấu hiệu càng cụ thể, thì càng tạo ra ít cảnh báo nhảm, nhưng càng khó phát hiện những biến thể của nó.

Ví dụ quen thuộc về signature-based IDS là EMERALD và nhiều sản phẩm thương mại khác.

#### 4.1.3 Nguyên lý hoạt động

Nguyên lý hoạt động của một hệ thống phòng chống xâm nhập được chia làm 5 giai đoạn chính: Giám sát mạng, Phân tích lưu thông, Liên lạc giữa các thành phần, Cảnh báo về các hành vi xâm nhập và cuối cùng có thể tiến hành Phản ứng lại tùy theo chức năng của từng IDS.



*Nguyên lý hoạt động của một hệ thống IDS*

- **Giám sát mạng** (Monitoring): Giám sát mạng là quá trình thu thập thông tin về lưu thông trên mạng. Việc này thông thường được thực hiện bằng các Sensor. Yêu cầu đòi hỏi đối với giai đoạn này là có được thông tin đầy đủ và toàn vẹn về tình hình mạng. Đây cũng là một vấn đề khó khăn, bởi vì nếu theo dõi toàn bộ thông tin thì sẽ tiêu tốn khá nhiều tài nguyên, đồng thời gây ra nguy cơ tắt nghẽn mạng. Nên cần thiết phải cân nhắc để không làm ảnh hưởng đến toàn bộ hệ thống. Có thể sử dụng phương án là thu thập liên tục trong khoảng thời gian dài hoặc thu thập theo từng chu kỳ. Tuy nhiên khi đó những hành vi bắt được chỉ là những hành vi trong khoảng thời gian giám sát. Hoặc có thể theo vết những lưu thông TCP theo gói hoặc theo liên kết. Bằng cách này sẽ thấy được những dòng dữ liệu vào ra được phép. Nhưng nếu chỉ theo dõi những liên kết thành công sẽ có thể bỏ qua những thông tin có giá trị về những liên kết không thành công mà đây lại thường là những phần quan trọng trong một hệ thống IDS, ví dụ như hành động quét cổng.
- **Phân tích lưu thông** (Analyzing): Khi đã thu thập được những thông tin cần thiết từ những điểm trên mạng. IDS tiến hành phân tích những dữ liệu thu thập được. Mỗi hệ thống cần có một sự phân tích khác nhau vì không phải môi trường nào cũng giống nhau. Thông thường ở giai đoạn này, hệ thống IDS sẽ dò tìm trong dòng traffic mạng

những dấu hiệu đáng nghi ngờ dựa trên kỹ thuật đối sánh mẫu hoặc phân tích hành vi bất thường. Nếu phát hiện ra dấu hiệu tấn công, các Sensor sẽ gửi cảnh báo về cho trung tâm để tổng hợp.

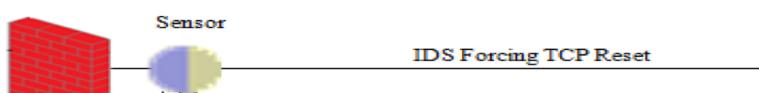
- **Liên lạc:** Giai đoạn này giữ một vai trò quan trọng trong hệ thống IDS. Việc liên lạc diễn ra khi Sensor phát hiện ra dấu hiệu tấn công hoặc Bộ xử lý thực hiện thay đổi cấu hình, điều khiển Sensor. Thông thường các hệ thống IDS sử dụng các bệ giao thức đặc biệt để trao đổi thông tin giữa các thành phần. Các giao thức này phải đảm bảo tính Tin cậy, Bí mật và Chịu lỗi tốt, ví dụ: SSH, HTTPS, SNMPv3 . . . Chẳng hạn hệ thống IDS của hãng Cisco thường sử dụng giao thức PostOffice định nghĩa một tập các Thông điệp để giao tiếp giữa các thành phần.

**Cảnh báo (Alert):** Sau khi đã phân tích xong dữ liệu, hệ thống IDS cần phải đưa ra được những cảnh báo. Ví dụ như:

- Cảnh báo địa chỉ không hợp lệ.
- Cảnh báo khi một máy sử dụng hoặc cố gắng sử dụng những dịch vụ không hợp lệ.
- Cảnh báo khi máy cố gắng kết nối đến những máy nằm trong danh sách cấm theo dõi ở trong hay ngoài mạng.
- ...

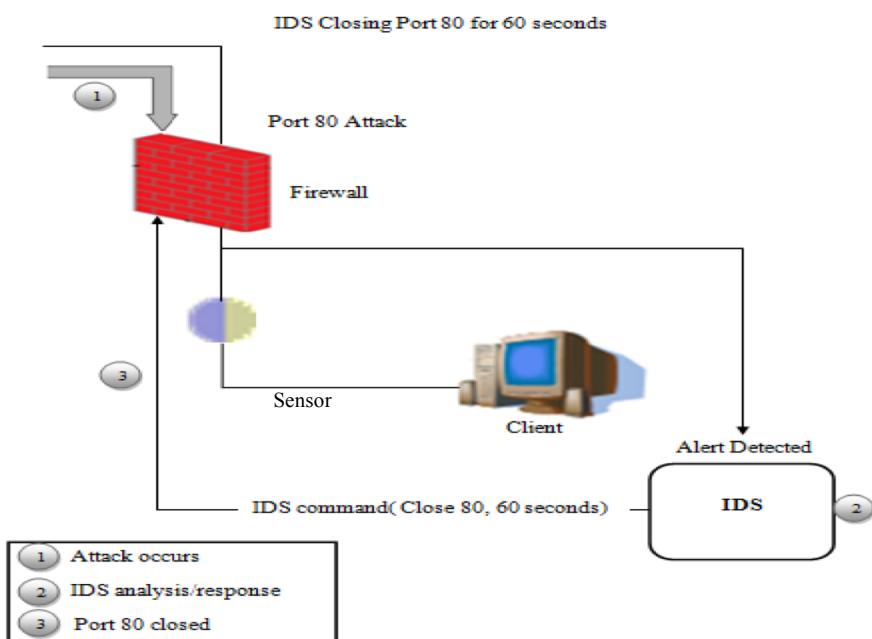
**Phản ứng (Response):** Trong một số hệ thống IDS tiên tiến hiện nay, sau khi các giai đoạn trên phát hiện được dấu hiệu tấn công, hệ thống không những cảnh báo cho người quản trị mà còn đưa ra các hành vi phòng vệ ngăn chặn hành vi tấn công đó. Điều này giúp tăng cường khả năng tự vệ của Mạng, vì nếu chỉ cần cảnh báo cho người quản trị thì đôi khi cuộc tấn công sẽ tiếp tục xảy ra gây ra các tác hại xấu. Một hệ thống IDS có thể phản ứng lại trước những tấn công phải được cấu hình để có quyền can thiệp vào hoạt động của Firewall, Switch và Router. Các hành động mà IDS có thể đưa ra như:

- Ngắt dịch vụ.
- Gián đoạn phiên.
- Cấm địa chỉ IP tấn công.
- Tạo log.



Client

IDS yêu cầu Firewall chặn port 80 trong 60s để chống lại các tấn công vào máy chủ Web cài IIS.



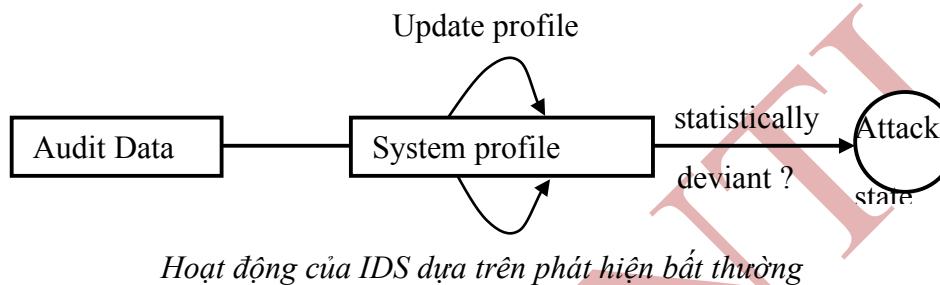
Hình 1.9 – IDS yêu cầu Firewall tạm dừng dịch vụ

IDS yêu cầu Firewall tạm dừng dịch vụ

#### 4.1.4 Hệ thống IDS dựa trên phát hiện bất thường

Hệ thống phát hiện bất thường giống các hệ thống IDS truyền thống ở chỗ nó cũng hướng đến việc kiểm soát và phát hiện sớm các dấu hiệu, các hành vi tấn công trong hệ thống mạng, từ đó cảnh báo cho nhà quản trị biết được những hiện tượng cần lưu ý. Tuy

nhiên xét về phương pháp hoạt động thì nó khác biệt so với các hệ thống IDS cũ. Nếu hệ thống IDS truyền thống thường sử dụng các mẫu (pattern) và kiểm soát các hành vi sử dụng sai đã được định nghĩa, thì phương pháp phát hiện bất thường hướng đến việc xây dựng profile về hoạt động của mạng ở trạng thái bình thường, từ đó so sánh, phát hiện và cảnh báo khi có những dấu hiệu khác thường xảy ra[8].



#### 4.1.4.1 Định nghĩa bất thường trong mạng

Bất thường trong mạng (BTTM) là thuật ngữ dùng để chỉ tình trạng hoạt động của hệ thống mạng hoạt động ngoài trạng thái bình thường. BTTM có thể phát sinh từ nhiều nguyên nhân, có thể là do một hoặc nhiều thiết bị trong mạng hỏng hóc, băng thông mạng bị quá tải, nhưng thường thấy hơn cả là do hệ thống thông tin đang bị xâm nhập trái phép hoặc đang bị tấn công.

Để phân biệt giữa trạng thái bình thường và trạng thái bất thường trong mạng, người ta sử dụng khái niệm activity profile (hồ sơ hoạt động). Một cách khái quát, activity profile mô tả hành vi của một đối tượng nào đó ở một số khía cạnh cụ thể. Thông thường khía cạnh là các tham số có thể tiến hành đo lường được. Người ta theo dõi các tham số này trong một thời gian nhất định, theo một đơn vị nào đó như phút, giờ, ngày, tuần . . . Hoặc có thể đo lường thời gian xảy ra hai sự kiện liên tiếp, ví dụ như thời gian log-in và log-out hệ thống, thời gian kích hoạt và kết thúc các ứng dụng . . .

Để phát hiện một profile là “bất thường”, người ta phải tiến hành xây dựng tập các profile mô tả hoạt động của hệ thống ở trạng thái “bình thường”. Dựa trên sự khác biệt của một tập các tham số trong profile, người ta có thể phát hiện ra BTTM.

*Các BTTM thông thường được phân thành 2 loại chính:*

- BTTM do hỏng hóc: Trong mạng này sinh ra các hiện tượng bất thường do một hay nhiều thành phần trong mạng bị sự cố, ví dụ như khi một máy chủ bị lỗi, thiết bị switch hay router gặp sự cố, broadcast storm, network paging . . . Các sự cố này nói chung không ảnh hưởng đến các thành phần khác trong mạng, chủ yếu là làm giảm hiệu năng hoạt động, hạn chế khả năng đáp ứng dịch vụ của hệ thống. Ví dụ như khi số lượng các yêu cầu đến một File Server hay Web Server quá lớn, các Server này sẽ gặp sự cố. Lỗi Network paging xảy ra khi một ứng dụng bị tràn bộ nhớ và tiến hành Phân trang bộ nhớ đến một File Server. Ngoài ra các loại BTTM còn xảy ra do các phần mềm bị lỗi, ví dụ như việc triển khai một giao thức không đúng, dẫn đến máy trạm liên tục gửi các gói tin nhỏ nhất làm tắc nghẽn mạng . . .
- BTTM liên quan đến các sự cố an ninh: Đây là loại BTTM phát sinh từ các mối đe dọa đối với hệ thống thông tin. Một ví dụ điển hình của loại BTTM này là tấn công từ chối dịch vụ DoS (Denial of Service), có thể mô tả như hành động ngăn cản những người dùng hợp pháp mất khả năng truy cập và sử dụng vào một dịch vụ nào đó. Cách tiến hành tấn công DoS bao gồm làm tràn ngập mạng, mất kết nối với dịch vụ . . . mà mục đích cuối cùng là máy chủ không thể đáp ứng được các yêu cầu sử dụng dịch vụ từ các máy trạm. BTTM còn xuất hiện khi có hiện tượng lây lan và bùng nổ các loại mã xấu, mã nguy hiểm trong mạng như virus, spy. Đôi khi hành vi dò quét trước khi tấn công cũng tạo ra nhiều gói tin với số lượng bất thường. Ngoài ra khi các chức năng có bản của mạng như DHCP, DNS bị làm ngưng hoạt động thì cũng tạo ra một số lượng lớn các yêu cầu không được đáp ứng làm giảm thiểu băng thông.

Một trong những nghiên cứu đầu tiên về hệ thống IDS dựa trên phát hiện bất thường là của Anderson. Trong báo cáo của Anderson, ông đưa ra cách phân loại 3 mối đe dọa chính, là:

- Xâm nhập từ bên ngoài (external penetrations): Hệ thống bị tấn công từ cá máy tính hoặc hệ thống không được xác minh.
- Xâm nhập từ bên trong (internal penetrations): Các máy tính được xác minh truy cập vào các dữ liệu không được phân quyền.

Lạm quyền (misfeasance): Sử dụng sai quyền truy cập vào hệ thống và dữ liệu.

#### 4.1.4.2 Kỹ thuật phát hiện bất thường

Để phát hiện bất thường trong mạng, người ta sử dụng một số kỹ thuật cụ thể, các kỹ thuật này có thể dùng tách biệt hoặc phối hợp với nhau. Có 3 kỹ thuật phát hiện cơ bản là:

Threshold Detection: Kỹ thuật này nhấn mạnh thuật ngữ “đếm”. Các mức ngưỡng về các hoạt động bình thường được đặt ra, nếu có sự bất thường nào đó như login với số lần quá quy định, số lượng các tiến trình hoạt động trên CPU, số lượng một loại gói tin được gửi vượt quá mức. . .

Self-learning Detection: Kỹ thuật này bao gồm hai bước, khi thiết lập hệ thống phát hiện tấn công, nó sẽ chạy ở chế độ tự học và thiết lập một profile mạng với các hoạt động bình thường. Sau thời gian khởi tạo, hệ thống sẽ chạy ở chế độ sensor theo dõi các hoạt động bất thường của mạng so với profile đã thiết lập. Chế độ tự học có thể chạy song song với chế độ sensor để cập nhật bản profile của mình nhưng nếu dò ra có tín hiệu tấn công thì chế độ tự học phải dừng lại tới khi cuộc tấn công kết thúc.

Anomaly protocol detection: Kỹ thuật này căn cứ vào hoạt động của các giao thức, các dịch vụ của hệ thống để tìm ra các gói tin không hợp lệ, các hoạt động bất thường là dấu hiệu của sự xâm nhập, tấn công. Kỹ thuật này rất hiệu quả trong việc ngăn chặn các hình thức quét mạng, quét cổng để thu thập thông tin của các hacker.

#### 4.1.4.3 Ưu nhược điểm của phát hiện bất thường

Phương pháp thăm dò bất thường của hệ thống rất hữu hiệu trong việc phát triển các cuộc tấn công như dạng tấn công từ chối dịch vụ. Ưu điểm của phương pháp này là có thể

phát hiện ra các kiểu tấn công mới, cung cấp các thông tin hữu ích bổ sung cho phương pháp do sự lạm dụng, tuy nhiên chúng có nhược điểm thường tạo ra một số lượng lớn các cảnh báo sai làm giảm hiệu suất hoạt động của mạng. Tuy nhiên vai trò của phương pháp này rất quan trọng, bởi một kẻ tấn công dù biết rõ về hệ thống cũng không thể tính toán được các hành vi nào là hành vi mà hệ thống coi là “bình thường”. Do đó đây sẽ là hướng được nghiên cứu nhiều hơn, hoàn thiện hơn để hệ thống chạy ngày càng chuẩn xác.

Ngoài IDS dựa trên phát hiện bất thường còn có thể phát hiện các cuộc tấn công từ bên trong, ví dụ như một người ăn cắp tài khoản của một người khác và thực hiện các hành vi không giống như chủ nhân của tài khoản đó thường làm, hệ thống IDS có thể nhận thấy các bất thường đó.

IDS dựa trên Misuse	IDS dựa trên phân tích hành vi
Là phương pháp truyền thống, sử dụng một tập các mẫu mô tả hành vi bất thường	Là phương pháp tiên tiến, không cần sử dụng tập mẫu
Không phát hiện được các dạng tấn công lạ, chẳng hạn như Zero-Day attack	Có khả năng phát hiện các cuộc tấn công mới
Biến thể của bất thường không được phát hiện	Không bị điểm yếu này do không sử dụng tập mẫu
Tỉ lệ False positive <sup>2</sup> thấp hơn	Tỉ lệ False positive thường cao
Tỉ lệ False negative <sup>3</sup> thường cao	Tỉ lệ False negative thấp hơn
Khi tập dữ liệu lớn sẽ bị overload	Không bị overload nhờ các phương pháp mô hình hóa dữ liệu và thuật toán heuristic

Dựa vào bảng trên chúng ta có thể thấy IDS dựa trên phát hiện bất thường mang tính trí tuệ và có nhiều ưu điểm hơn so với các hệ thống IDS truyền thống. Tuy nhiên, để tăng cường tính chính xác của cảnh báo thì nên có sự kết hợp giữa IDS bất thường và IDS kiểu cũ.

Cách nhận dạng các kiểu tấn công của IDS dựa trên phát hiện bất thường:

STT	Dạng tấn công	Cách phát hiện
1	Xâm nhập leo thang	Phát hiện bằng các profile bất thường hoặc sự vi phạm chính sách an ninh
2	Tấn công giả dạng	Phát hiện bằng các profile bất thường hoặc sự vi phạm các chính sách an ninh
3	Thâm nhập vào hệ thống điều khiển	Phát hiện bằng cách giám sát một số hành vi đặc biệt
4	Rò rỉ thông tin	Phát hiện bằng cách giám sát việc sử dụng tài nguyên bất thường
5	Tấn công từ chối dịch vụ	Phát hiện bằng cách giám sát việc sử dụng tài nguyên bất thường
6	Mã độc hại	Phát hiện các hành vi bất thường, vi phạm chính sách an ninh, sử dụng các đặc quyền bất thường

**False positive<sup>2</sup>:** Là trường hợp hệ thống IDS sinh ra các cảnh báo khi luồng dữ liệu bình thường đi qua, không có tấn công xâm nhập. Loại cảnh báo sai này hầu hết các hệ thống IDS đều có. Khi tỉ lệ này quá cao sẽ gây nhiễu cho người quản trị.

**False negative<sup>3</sup>:** Có ý nghĩa ngược lại với False positive. Cảnh báo này xảy ra khi một IDS không nhận ra được những cuộc tấn công thật sự. Nguyên nhân của False negative có thể là do thông tin về dạng tấn công chưa được IDS biết, hoặc do chính sách an ninh và điều khiển

của người quản trị. Hầu hết các hệ thống IDS có khuynh hướng tối thiểu hóa False negative. Tuy nhiên, rất khó loại trừ toàn bộ False negative. Hơn nữa khi hệ thống có một vài False negative, người quản trị có xu hướng thắt chặt việc kiểm soát và làm tăng số lượng false positive. Do đó cần có sự tính toán cân bằng hợp lý.

#### 4.1.4.4 Dữ liệu phát hiện bất thường

Nguồn dữ liệu đóng vai trò quan trọng trong phương pháp phát hiện bất thường. Số liệu chính xác về tình trạng hoạt động của mạng sẽ có tính chất quyết định đến việc các bất thường có được phát hiện hay không. Do bản chất của phương pháp phát hiện bất thường là mô hình hóa và lập một hồ sơ về trạng thái bình thường rồi từ đó so sánh để phân biệt khi có sự cố xảy ra, nên nếu số liệu phân tích được cung cấp càng đầy đủ và chuẩn xác thì hiệu quả hoạt động của các thuật toán phát hiện bất thường sẽ càng cao. Sau đây ta đi liệt kê một số nguồn dữ liệu thường được sử dụng:

##### 4.4.4.1 Network Probes

Network Probes là những công cụ chuyên dụng dùng để đo lường các tham số mạng. Một ví dụ đơn giản về Network Probes là 2 lệnh ping và tracerouter, các lệnh này dùng để đo độ trễ (end-to-end delay), tỉ lệ mất gói tin (packet loss), bước truyền (hop), . . .

Network Probes có thể cung cấp các số liệu tức thời, phương pháp này không yêu cầu sự phối hợp của nhà cung cấp dịch vụ. Tuy nhiên, Network Probes có thể không hoạt động nếu như trên Firewall đặt các tập luật ngăn chặn loại traffic này. Ngoài ra các gói tin mà giao thức này sử dụng thường được các thiết bị mạng đổi xử một cách đặc biệt không giống như các gói tin bình thường khác, do vậy các số liệu của Network Probes cần được tinh chỉnh thêm.

```
[root@server] ping 67.220.210.150
ping 67.220.210.150 with 64 bytes of data
64 bytes from 67.220.210.150: icmp_seq=1 ttl=52 time=87.7 ms
64 bytes from 67.220.210.150: icmp_seq=2 ttl=52 time=95.6 ms
64 bytes from 67.220.210.150: icmp_seq=3 ttl=52 time=85.4 ms
64 bytes from 67.220.210.150: icmp_seq=4 ttl=52 time=95.8 ms
64 bytes from 67.220.210.150: icmp_seq=5 ttl=52 time=87.0 ms
64 bytes from 67.220.210.150: icmp_seq=6 ttl=52 time=97.6 ms
```

#### 4.4.4.2 Kỹ thuật lọc gói tin

Có một kỹ thuật được dùng để cung cấp dữ liệu cho các thuật toán phát hiện bất thường đó là kỹ thuật lọc gói tin để thống kê luồng (packet filtering for flow-based statistics). Luồng thông tin được dẫn qua một bộ lọc để lấy mẫu, các IP header của các gói tin trong những thời điểm khác nhau tại các địa điểm khác nhau trong mạng được ghi lại.

Việc tổng hợp các IP header cho phép cung cấp các thông tin chi tiết về tình trạng hoạt động của hệ thống mạng. Các luồng thông tin được giám sát, một luồng được xác định bằng địa chỉ nguồn-dịch và cổng nguồn-dịch. Phương pháp lọc gói tin cho phép có được các thống kê chính xác về giao dịch trong mạng.

#### 4.1.4.3 Dữ liệu từ các giao thức định tuyến

Các giao thức định tuyến cũng là một nguồn cung cấp dữ liệu cho thuật toán phát hiện bất thường trong mạng. Trong quá trình định tuyến, các router liên lạc với nhau để trao đổi các

thông tin về trạng thái đường truyền ví dụ như: băng thông, độ trễ, kết nối có bị tắt nghẽn hay không. Ví dụ với giao thức định tuyến OSPF (Open-Shortest Path First), tại mỗi router có các bảng thông số mô tả về hình trạng mạng cũng như trạng thái các đường truyền.

#### 4.1.4.4 Dữ liệu từ các giao thức quản trị mạng

Các giao thức quản trị mạng cung cấp các thông kê về lưu thông mạng. Những giao thức này có các tham số có thể giám sát hoạt động của thiết bị mạng một cách hiệu quả. Các tham số không cung cấp trực tiếp các thông tin đo lường về giao thông mạng nhưng có thể dùng để nhận dạng các hành vi trên mạng, do đó phù hợp với phương pháp phát hiện bất thường.

SNMP: là giao thức hoạt động theo mô hình client-server có mục đích quản lý, giám sát, điều khiển các thiết bị mạng từ xa. SNMP hoạt động dựa trên giao thức UDP. SNMP server thu thập các thông tin gửi từ agent. Tuy nhiên nó không có chức năng xử lý thông tin. SNMP server lưu trữ các thông tin này trong một cơ sở dữ liệu gọi là MIB (Management Information Base). Các giá trị trong CSDL này chứa các thông tin được ghi nhận khi các thiết bị mạng thực hiện các chức năng khác nhau.

Từng thiết bị mạng có một tập các giá trị MIB tương ứng với chức năng của nó. Các giá trị MIB được xác định dựa trên loại thiết bị và các giao thức mạng hoạt động dựa trên các thiết bị đó. Ví dụ như một switch sẽ có các giá trị MIB đo lường lưu thông mạng ở mức đường truyền (link-level) trong khi một router sẽ có các tham số ở mức mạng (network-level) cung cấp các thông tin về tầng mạng trong mô hình OSI. Ưu điểm của việc sử dụng SNMP là tính chuẩn hóa do SNMP đã được chấp nhận và triển khai rộng rãi trên các thiết bị khác nhau. Do tính đầy đủ và có chọn lọc của dữ liệu nên SNMP là nguồn thông tin đầu vào rất quan trọng cho các thuật toán phát hiện bất thường trong mạng.

#### 4.4.5 Các phương pháp phát hiện bất thường

##### 4.4.5.1 Xác suất thống kê

Phương pháp xác suất thống kê được sử dụng ở nhiều trong các hệ thống phát hiện bất thường. Như tên gọi của nó, phương pháp này sử dụng mô hình Xác suất để mô tả tất cả các

hoạt động trong Hệ thống mạng. Mục tiêu của phương pháp này là thiết một mô hình dữ liệu phù hợp để lưu trữ tri thức về tính bình thường của lưu thông mạng, dựa vào đó có thể đánh giá được tính bất thường tại từng thời điểm cụ thể.

Trong phương pháp này, hệ thống quan sát hành vi của các đối tượng và lập profile về tập hành vi đó. Profile thông thường bao gồm các đại lượng đo lường về mật độ, cường độ hoạt động, đo lường theo từng loại hoạt động, các thông số kỹ thuật (như sử dụng CPU, RAM) .

Một số hệ thống phát hiện bất thường dựa trên xác suất:

#### a. Haystack

Haystack là một trong những hệ thống phát hiện bất thường đầu tiên sử dụng phương pháp xác suất thống kê. Haystack sử dụng cả chiến lược phát hiện bất thường trên máy trạm và trên một vùng mạng, mô hình hóa các tham số như là các biến độc lập và ngẫu nhiên. Đối với từng yếu tố quan sát, Haystack định nghĩa một khoảng các giá trị được coi là “bình thường”. Trong một phiên, khi yếu tố quan sát có giá trị đi ra ngoài “khoảng bình thường” thì hệ thống sẽ tính điểm dựa trên phân bố xác suất và một cảnh báo được sinh ra nếu điểm số tính quá cao. Ngoài ra đối với từng người sử dụng, Haystack còn lưu trữ các thông tin về các quyền được cấp phép và giám sát hành vi. Nếu hành vi vượt ra ngoài các quyền đó thì hệ thống sẽ được coi là bất thường. Điểm yếu của Haystack là nó được thiết kế để chạy offline, không thể giám sát thời gian thực do không đảm bảo hiệu năng xử lý.

#### b. SPADE

SPADE (Statistical Packet Anomaly Detection Engine) là một hệ thống phát hiện bất thường dựa trên thống kê, SPADE là nghiên cứu đầu tiên đưa khái niệm “chỉ số bất thường” (anomaly score) nhằm phát hiện các dấu hiệu tấn công. Phương pháp này sử dụng cách tiếp cận tính toán tần suất xuất hiện của yếu tố quan sát để tính ra “chỉ số bất thường”, thay vì thống kê p sự kiện trong q đơn vị thời gian như các phương pháp truyền thống.

Phương pháp này sử dụng một hàm chỉ số  $A(x)$  để đánh giá mức độ bất thường của sự kiện  $x$ . Giá trị  $A(x)$  được tính bằng hàm logarit của phân phối xác suất xảy ra sự kiện  $x$ . Để hỗ

trợ việc lưu trữ dữ liệu và tính toán trong trường hợp số lượng thông số lớn, người ta sử dụng mạng Bayes để mô tả mối liên hệ phức tạp giữa các thông số. Từ đó có thể tính xác suất hợp bằng cách xác suất có điều kiện và xác suất không điều kiện của tổ hợp ít thông số hơn.

Nguyên lý hoạt động của phương pháp này như sau:

Giả sử rằng chúng ta đã có một cơ sở dữ liệu thống kê về hoạt động mạng bình thường, bao gồm các phân bố xác suất về các sự kiện. Khi nhận được một biến cõi  $x$ , ta dễ dàng tính ra được  $P(x)$  là xác suất xuất hiện  $x$  hoạt động bình thường của mạng là bao nhiêu. Từ đó có thể tính ra chỉ số bất thường  $A(x)$  bằng cách thực hiện làm Logarit trên  $P(x)$ :

$$A(x) = -\log(P(x))$$

Hàm EC là hàm đánh giá sự kiện  $x$  có phải là bất thường hay không:

$$EC(x, I) = \begin{cases} \text{"Bất thường" nếu } A(x) > I \\ \text{"Bình thường" nếu } A(x) \leq I \end{cases}$$

Ở đây cần một tri thức  $I$  được cung cấp thêm nhằm đánh giá đâu là ngưỡng để đánh giá một sự kiện là bất thường.  $A(x) > I$ , sự kiện  $x$  là bất thường,  $A(x) \leq I$ , sự kiện  $x$  là bình thường.

Trong trường hợp hành vi bất thường được mô tả bao gồm một tập  $X$  các sự kiện  $x$ , chẳng hạn Footprint của một hành vi dò quét cổng được mô tả bằng việc liên tục xuất hiện các gói tin với cổng lạ, thì hàm đánh giá là:

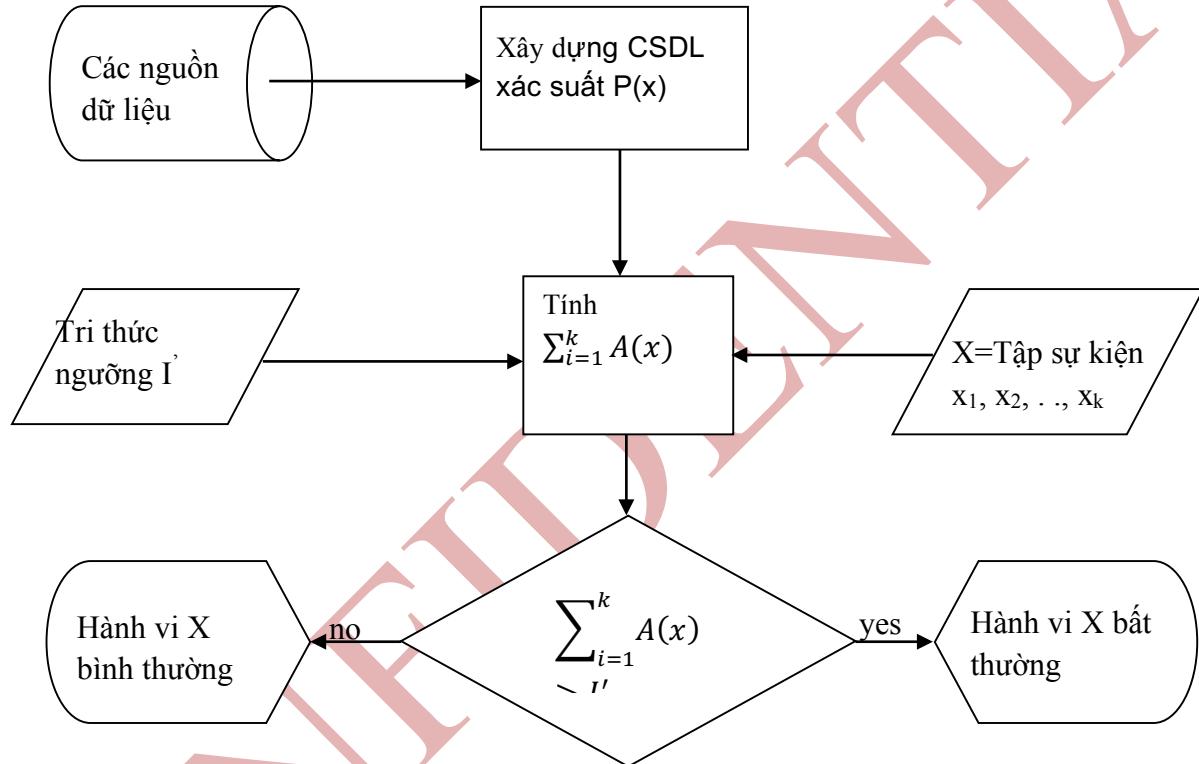
$$EC(x_1, x_2, \dots, x_k, I') = \{\text{bình thường, bất thường}\} \quad (*)$$

Hàm  $EC()$  có thể là một hàm phức tạp mô tả sự liên hệ giữa các sự kiện trong bản thân một hành vi. Tuy nhiên, để đơn giản hóa, trong hầu hết các trường hợp hàm  $EC()$  là một hàm tổng. Công thức (\*) có thể tính bằng:

$$EC(x, I) = \begin{cases} \text{"Bất thường" nếu } \sum_{i=1}^k A(x_i) > I' \\ \text{"Bình thường" nếu } \sum_{i=1}^k A(x_i) \leq I' \end{cases}$$

Ở đây sự kiện x bao gồm nhiều tham số,  $x=\{e_1, e_2, \dots, e_n\}$  trong đó  $e_i$  là thuộc tính mạng mà ta đang xét. Các thuộc tính này có thể lấy từ nhiều nguồn dữ liệu khác nhau.

Như vậy, ý tưởng chung về hệ thống xâm nhập bất thường dựa trên xác suất thống kê có thể mô tả bằng sơ đồ sau:



Mô hình cơ bản hệ thống Phát hiện xâm nhập bất thường bằng xác suất thống kê

CƠ  
BẢN

Hướng tiếp cận này khá đơn giản, tuy nhiên, một vấn đề đặt ra là trong hệ thống thực tế mỗi một sự kiện được đánh giá bằng nhiều tham số, với mỗi tham số lại có không gian mẫu lớn thì việc lưu trữ và tính toán xác suất sẽ quá tải. Để khắc phục nhược điểm này, người ta sử dụng một mô hình ước lượng nhằm tính gần đúng xác suất hợp  $P(e_1, e_2, \dots, e_n)$  bằng các xác suất đơn giản hơn:

$$P(x) = \psi(P(x_1), P(x_2), \dots, P(x_t))$$

Để có được mô hình ước lượng này, người ta thường sử dụng Mạng Bayes. Mạng Bayes mô tả mối liên hệ giữa các biến cố trong một hệ thống biến cố. Bằng cách lưu trữ các xác suất đơn và xác suất có điều kiện để mô tả Mạng Bayes, ta có thể tính ra được xác suất hợp  $P(x)$ .

Phát hiện bất thường dựa trên thống kê có ưu điểm là tính bao quát hệ thống và dễ triển khai, thực hiện. Tuy nhiên vấn đề lớn nhất là khi số yếu tố quan sát tăng lên hoặc không gian quan sát phân bố thưa, việc tính toán các xác suất hợp trở nên không chính xác và kém hiệu quả. Phương pháp này thường có tỷ lệ cảnh báo sai khá cao. Nhược điểm còn bộc lộ khi thủ phạm có trình độ cao có thể bí mật đào tạo cho hệ thống IDS dần dần chấp nhận các hành vi bất thường – bình thường sao cho phù hợp cũng là một bất đề lớn. Ngoài ra hệ thống phát hiện bất thường dựa trên xác suất cần có một dữ liệu đầy đủ về các phân bố xác suất, tuy nhiên việc giám sát được toàn bộ hệ thống mạng và các hành vi trên nó là rất khó khăn.

### c. NIDES

NIDES (Next Generation Intrusion Detection Expert System) cải tiến từ hệ thống IDES, được xây dựng bởi viện nghiên cứu Stanford. NIDES là một trong số ít những hệ thống IDS

có thể giám định thời gian thực. NIDES phân tích định kỳ hệ thống bằng cách xây dựng các profile bao gồm nhiều giá trị đặc trưng cho hệ thống. Các trọng số được gán cho từng bản ghi, trong đó cứ 30 ngày thì giá trị trọng số giảm đi một nửa, bằng cách này NIDES phân biệt được những dữ kiện đã xảy ra từ lâu với những dữ kiện vừa mới xảy ra. Tuy nhiên nhược điểm của phương pháp này là chỉ thống kê trên từng yếu tố quan sát nên không phát hiện ra được các cuộc tấn công ảnh hưởng trên diện rộng, tác động đến nhiều thành phần khác nhau của hệ thống.

#### 4.1.5.2 Máy trạng thái hữu hạn

Người ta có thể dùng Mô hình máy trạng thái hữu hạn FSM (Finite State Machine) để giải quyết bài toán phát hiện BTTM. Theo hướng này, các FSM sẽ xây dựng chuỗi các hành vi diễn ra trong trạng thái hoạt động bình thường, từ đó phát hiện ra quá trình xuất hiện lỗi. Dựa trên các số liệu đã được ghi lại trước đó, người ta sẽ xây dựng được mô hình FSM theo xác suất về các sự cố trên mạng. Từ đó, FSM không chỉ tập trung vào việc phát hiện ra các sự cố mạng mà còn giải quyết được bài toán xác định nguyên nhân dẫn đến sự cố. Các chuỗi báo động (sequence of alarm) ở các điểm khác nhau trên mạng sẽ được ghi nhận thành trạng thái của máy.

Một máy trạng thái hữu hạn A được định nghĩa bằng tập  $A = (A, \Sigma, q_0, \delta, F)$  trong đó:

- Q: tập trạng thái có thể có
- $\Sigma$ : tập ngôn ngữ hữu hạn
- $q_0 \in Q$ : trạng thái bắt đầu
- $\delta$ : hàm chuyển đổi  $\delta: Q \times \Sigma \rightarrow Q$
- $F \subseteq Q$ : tập các trạng thái kết thúc

FSM được dùng để mô hình hóa trạng thái hoạt động bình thường trong mạng, ví dụ như mô hình hóa các giao thức mạng. Các giao thức mạng sẽ được thể hiện bằng FSM, luồng dữ liệu đi qua sẽ được kiểm tra bởi các FSM để phát hiện ra những kết nối không tuân theo chuẩn. Ví dụ kết nối TCP SYN sẽ được mô hình hóa như sau:

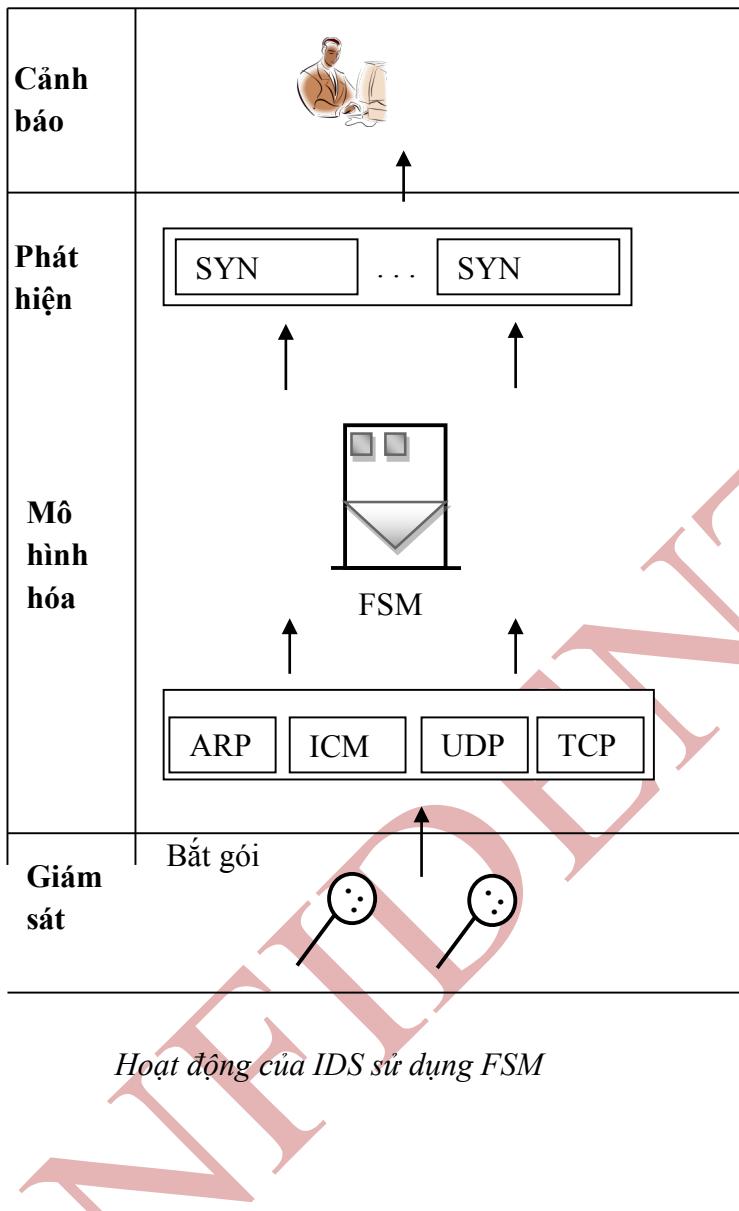


Việc phát hiện sự kiện bất thường bằng máy trạng thái hữu hạn dựa trên các đặc điểm như sau:

- ✓ *Tính đơn nhát (Atomicity)*: Các sự kiện phải được hoàn thành. Ví dụ như mỗi kết nối được coi như một đối tượng, một thực thể độc lập và được theo dõi để phát hiện bất thường
- ✓ *Tính bền vững (Consistency)*: Các hệ thống phải đưa hệ thống từ trạng thái bền vững này qua trạng thái bền vững khác.
- ✓ *Tính phân tách (Isolation)*: Mỗi sự kiện xảy ra mà không bị can thiệp bởi một sự kiện khác.

Từ những đặc điểm trên, FSM mô tả các sự kiện và phát hiện bất thường dựa trên sự khác nhau giữa sự kiện thực tế và sự kiện đã được mô tả.

Ưu điểm của phương pháp này là có cái nhìn nguyên nhân – kết quả đối với bất thường, từ đó phân định được bất thường có phải tấn công không. Tuy nhiên, phương pháp này có điểm yếu là rất tốn tài nguyên để thực hiện. Ngoài ra, nó cũng yêu cầu có tập dữ liệu tương đối đầy đủ về hoạt động mạng. Khi số lượng node tăng cao, cần thiết phải có các máy hiệu năng lớn để tính toán. Do đó các phương pháp này gần như không được triển khai trong thực tế.



#### 4.1.5.3 Phát hiện bất thường bằng mạng Nơ-ron

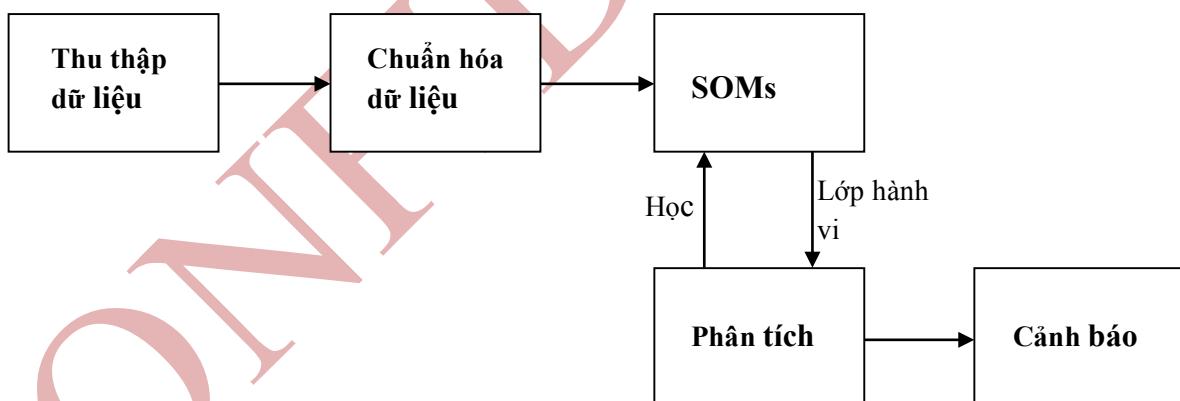
Hệ thống IDS sử dụng mạng Nơ-ron thường là host-based IDS, tập trung vào việc phát hiện các thay đổi trong hành vi của chương trình như là dấu hiệu bất thường. Theo cách tiếp cận này, mạng Nơ-ron sẽ học và dự đoán hành vi của người sử dụng và các chương trình tương ứng. Ưu điểm của mạng Nơ-ron là dễ dàng thích ứng với các kiểu dữ liệu không đầy đủ, dữ liệu với độ chắc chắn không cao, đồng thời phương pháp này cũng có khả năng đưa ra các kết luận mà không cần cập nhật tri thức thường xuyên. Điểm yếu của mạng Nơ-ron là tốc độ xử lý do hệ thống cần thu thập dữ liệu, phân tích và điều chỉnh từng Nơ-ron để cho kết

quả chính xác. Một số hệ thống IDS điển hình như: IDS sử dụng mạng Nơ-ron lan truyền ngược trong nghiên cứu của Ghost hay mạng Nơ-ron hồi quy trong nghiên cứu của Elman .

Một hướng khác để giải quyết vấn đề bất thường là sử dụng Bản đồ tự tổ chức SOM (Self Organizing Maps) như trong nghiên cứu của Ramadas. SOM được sử dụng nhằm mục đích đào tạo và phát hiện hành vi bất thường. SOM, còn được biết đến là SOFM (Self Organizing Feature Map) là một trong những mô hình biến dạng của mạng Nơ-ron. SOM được Kohonen phát triển vào đầu những năm 80, nên cũng thường được gọi là mạng Kohonen. SOM thường được dùng để học không có hướng dẫn (unsupervised learning).

Học không hướng dẫn dùng SOM cung cấp một phương thức đơn giản và hiệu quả để phân lớp các tập dữ liệu. SOM cũng được xem là một trong những hướng tiếp cận tốt cho việc phân lớp tập dữ liệu theo thời gian thực bởi tốc độ xử lý cao của thuật toán và tỷ lệ hội tụ nhanh khi so sánh với các kỹ thuật học khác.

Trong hệ thống phát hiện bất thường sử dụng SOM, người ta thiết lập các mạng nhằm phân lớp các hành vi, từ đó phát hiện ra các hành vi nghi vấn. Sơ đồ khái của giải thuật này như sau:



*IDS dựa trên SOM*

Đầu tiên các dữ liệu về mạng cần phân tích phải được thể hiện ở dạng vectơ các tham số đặc trưng. Tiếp theo các vectơ này được lưu trữ trong một input vectơ để tiến hành phân

lớp. Việc phân lớp này tiên hành lặp đi lặp lại cho đến khi hội tụ. Sau đó với các SOMs đã xây dựng được ta có thể tiến hành phân tích để xác định “khoảng cách” giữa hành vi đang xét với hành vi “bình thường”. Nếu khoảng cách này ra ngoài ngưỡng cho phép thì tiến hành cảnh báo.

#### 4.1.5.4 Phát hiện bất thường bằng Hệ chuyên gia

Phương pháp này có tên gọi là Rule-based Detection (Phát hiện dựa trên tập luật). Đây là một trong những hướng tiếp cận đầu tiên để giải quyết vấn đề phát hiện bất thường trong mạng. Phương pháp Rule-base này dựa trên Hệ chuyên gia, cần có một cơ sở dữ liệu đồ sộ bao gồm các luật để mô tả hành vi bất thường để phát hiện lỗi trong hệ thống. Các hệ thống Rule-based này trong thực tế không được sử dụng nhiều do hệ thống chạy quá chậm không thể đáp ứng thời gian thực, đồng thời cần phải có trước tri thức về triệu chứng của các cuộc tấn công. Một số triệu chứng như: mạng bị quá tải, số lượng kết nối TCP nhiều bất thường, thông lượng của các thiết bị đạt tới mức độ tối đa . . .

Phương pháp Rule-based phụ thuộc rất lớn vào kinh nghiệm của người quản trị vì khi hệ thống mạng có sự thay đổi và tăng trưởng về mô hình thì tập luật cũng phải thay đổi theo.

Phương pháp Rule-based bao gồm các bước sau:

Bước 1: Gia thiết rằng các sự kiện không xảy ra theo một trình tự ngẫu nhiên mà theo các khuôn dạng cho trước

Bước 2: Sử dụng các luật qui nạp theo thời gian để mô tả hành vi bình thường của người sử dụng

Bước 3: Các luật được chỉnh sửa và chỉ có những luật có mức *entropy*<sup>4</sup> thấp mới lưu lại trong tập luật.

Bước 4: Nếu chuỗi các sự kiện phù hợp với vé trái của luật, thì sẽ tiếp tục so sánh sự kiện tiếp theo để xác định bất thường nếu nó không nằm trong phần vé phải của luật.

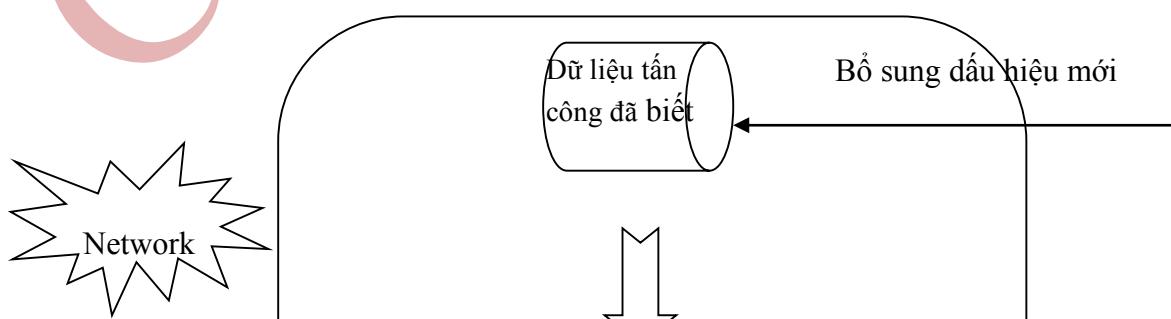
Ví dụ có luật là: E1 ->E2 -> E3  $\Rightarrow$  (E4=95%, E5=5%), nghĩa là nếu thấy liên tiếp các sự kiện E1, E2, E3 thì xác suất xảy ra sự kiện E4 là 95%, E5 là 5%.

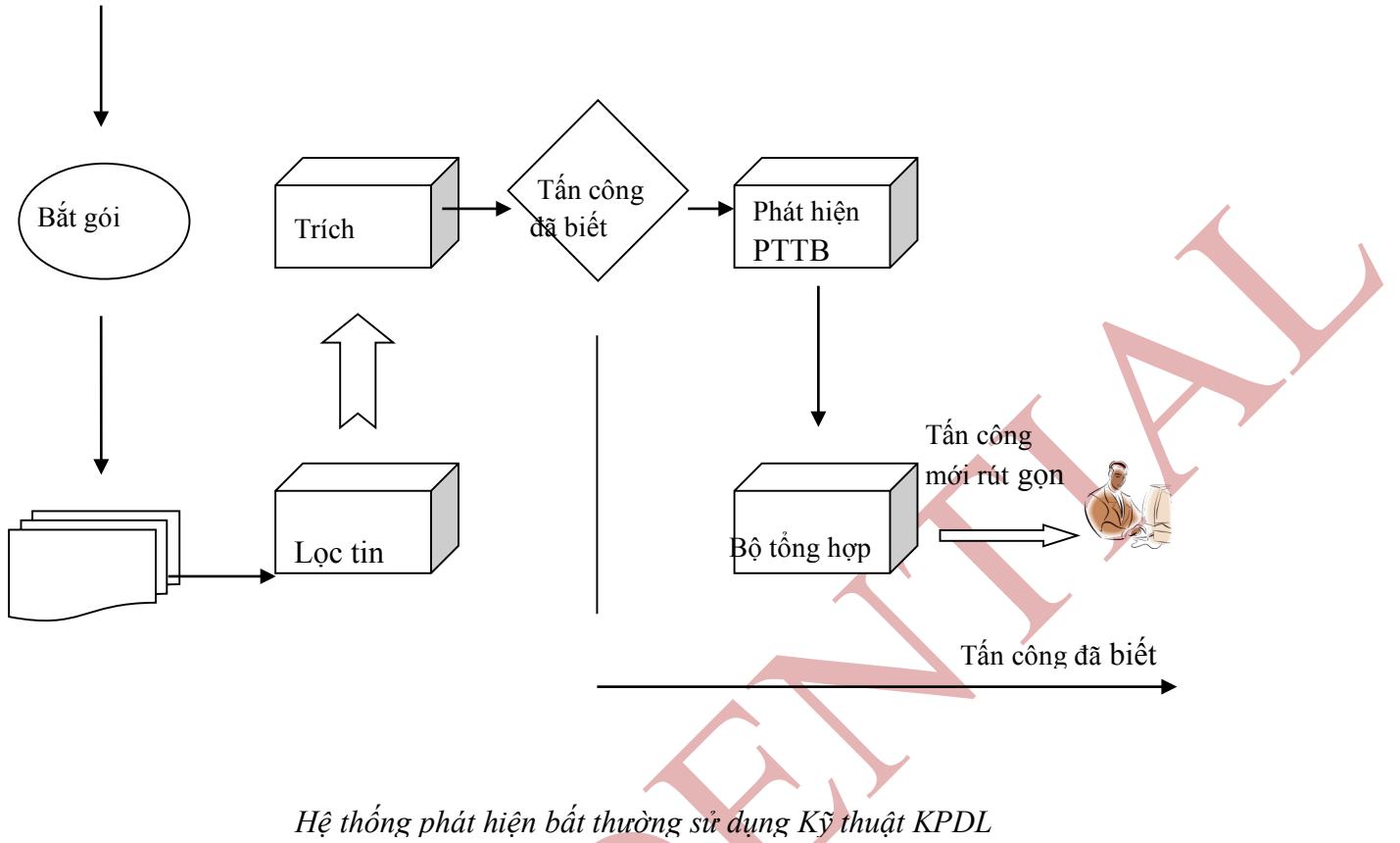
#### 4.1.5.5 Phát hiện bất thường bằng kỹ thuật khai phá dữ liệu

So với một số kỹ khác như Xác suất thống kê, Máy trạng thái thì Khai phá dữ liệu (KPDL) có một số ưu thế rõ rệt: KPDL có thể sử dụng với các CSDL chứa nhiều nhiễu, dữ liệu không đầy đủ hoặc biến đổi liên tục, mức độ sử dụng chuyên gia không quá thường xuyên. Dựa trên các ưu thế đó, KPDL gần đây cũng được các nhà nghiên cứu áp dụng vào Hệ thống phát hiện xâm nhập trái phép.

Ưu điểm vượt trội của phương pháp này là khả năng xử lý khối lượng dữ liệu lớn, có thể phục vụ cho các hệ thống thời gian thực. Hệ thống IDS sử dụng KPDL cũng được chia theo 2 hướng chính là phát hiện dựa trên hành vi lạm dụng và phát hiện bất thường. Trong hướng phát hiện dựa trên hành vi lạm dụng, các mẫu trong tập dữ liệu được gán nhãn là “bình thường” hay “bất thường”. Một thuật toán học sẽ được đào tạo trên tập dữ liệu được gán nhãn. Kỹ thuật này sẽ được áp dụng tự động trên các dữ liệu đầu vào khác nhau để phát hiện tấn công. Các nghiên cứu theo hướng này chủ yếu dựa vào việc phân lớp các hành vi sử dụng các thuật toán KPDL khác nhau như: Phân cụm, Phân tích luật tích hợp. Ưu điểm của hướng này là khả năng phát hiện chính xác các tấn công đã biết đến và các biến thể của nó với độ chính xác cao. Nhược điểm là nó không thể phát hiện các tấn công mới mà chưa có mẫu hay biến thể nào được quan sát.

Đối với hướng tiếp cận bất thường, gần đây trong lĩnh vực KPDL, người ta thường nhắc đến Bài toán phát hiện phần tử tách biệt (Outlier Detection – phần tử ngoại lai hay phần tử tách rời). Mục tiêu của bài toán này là phát hiện phần tử tách biệt, với dữ liệu là tập thông tin quan sát hoạt động mạng, còn phần tử tách biệt tương ứng với các dạng tấn công. Các thuật toán Phát hiện phần tử tách biệt, cũng thừa hưởng ưu điểm của phương pháp KPDL, đó là khả năng hoạt động ổn định trong tập dữ liệu, đó là khả năng hoạt động ổn định trong tập dữ liệu nhiễu, dữ liệu không đầy đủ, dữ liệu khối lượng lớn và có tính chất phân bố.



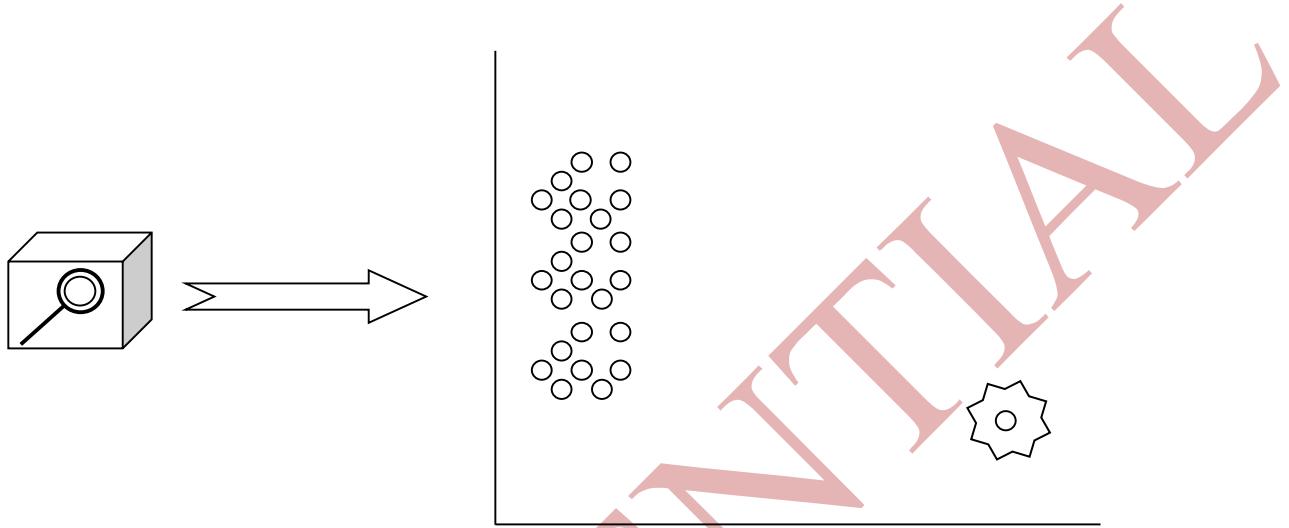


Hệ thống phát hiện bất thường dựa trên kỹ thuật KPDL lấy ý tưởng chủ đạo là sử dụng các giải thuật *phân tử tách biệt*. Bên cạnh đó, hệ thống còn có một số cải tiến như sử dụng *bộ lọc* các kiểu tấn công đã biết dấu hiệu (các dấu hiệu này được hệ thống tự học), sử dụng một bộ *tổng hợp* nhằm rút gọn cảnh báo lên *chuyên gia*. Đồng thời bộ *tổng hợp* này cũng có chức năng xây dựng luật rút gọn để bổ sung tri thức cho hệ thống. Module *tổng hợp* được xây dựng dựa trên một số kỹ thuật khác của KPDL là kỹ thuật *tổng hợp* (Summarization). Ngoài ra hệ thống còn có các thành phần tương tự như các hệ thống IDS khác như Module lọc tin, Module trích xuất thông tin.

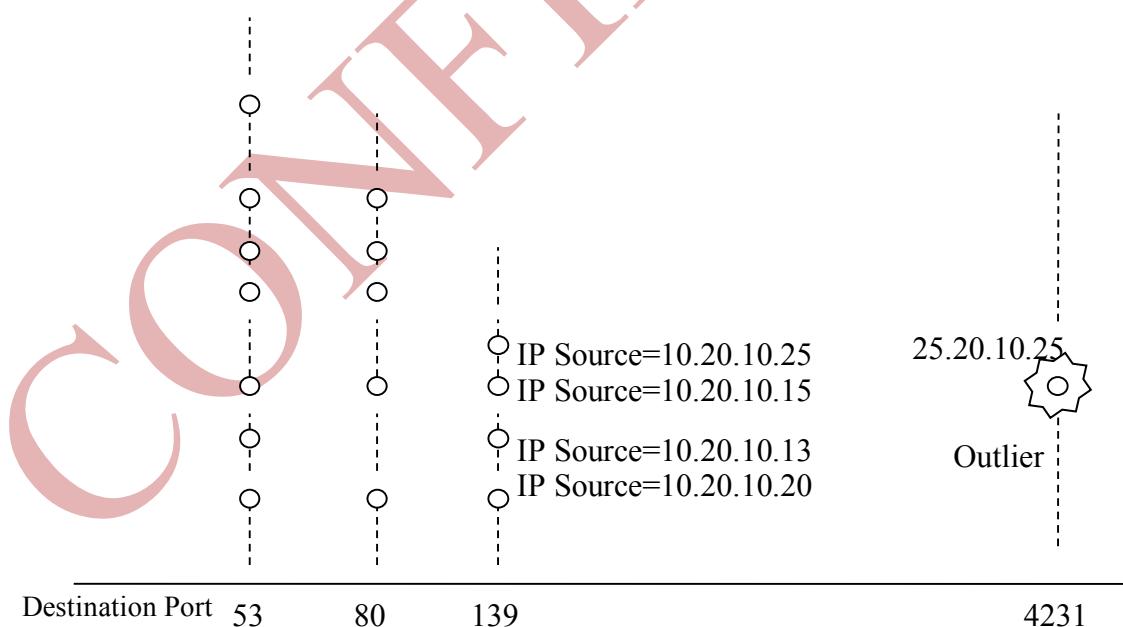
#### a. Khái niệm phân tử tách biệt

Định nghĩa phân tử tách biệt theo định nghĩa của Hawkins năm 1980 cho rằng: *Phân tử tách biệt là một quan sát có độ sai lệch lớn hơn so với các quan sát khác và do đó có thể nghi ngờ nó được sinh ra từ một cơ chế khác*.

Ta biết rằng các sự kiện khác biệt thường mang lại thông tin nhiều hơn so với các sự kiện bình thường. Do đó việc phát hiện phân tử tách biệt là cần thiết trong nhiều lĩnh vực khác nhau. Dựa trên các yếu tố cấu thành nên phân tử tách biệt, ta chia chúng thành 2 loại: Phân tử tách biệt một chiều và phân tử tách biệt nhiều chiều.



Ảnh xạ bài toán Phát hiện bất thường về bài toán Phát hiện PTTB



Kết nối bất thường là một phân tử tách biệt

### ✓ **Phần tử tách biệt một chiều:**

Giả sử có  $\bar{x}$  là trung vị và  $S$  là độ lệch chuẩn của một phân bố dữ liệu. Một quan sát được coi là tách biệt nếu nó nằm ngoài khoảng sau:

$$(\bar{x} - kS, \bar{x} + kS)^{(*)}$$

Trong đó  $k$  thường lấy giá trị là 2, 3. Việc lựa chọn giá trị của  $k$  phụ thuộc vào phân bố chuẩn được mong đợi chiếm 95,45% hay 99,75% dữ liệu.

Từ công thức <sup>(\*)</sup>, quan sát  $x$  được coi là tách biệt nếu như:

$$\frac{x - \bar{x}}{S} > k$$

### ✓ **Phần tử tách biệt nhiều chiều:**

Tổng quát hóa phần tử tách biệt một chiều, chúng ta có phần tử tách biệt nhiều chiều. Trong thực tế, một sự kiện diễn ra bao gồm nhiều yếu tố quan sát khác nhau. Ví dụ như sự kiện kiểm tra hành vi quét cổng sẽ bao gồm các yếu tố quan sát như Source IP, Destination IP, Source Port, Destination Port . . . Bài toán phát hiện phần tử tách biệt được thực hiện trên một tập dữ liệu  $D$  với  $p$  thuộc tính và  $n$  mẫu. Trong một mô hình phân lớp các đối tượng, cần phải xác định các phần tử tách biệt dựa trên các kiểm tra mẫu.

Tuy nhiên phần tử tách biệt nhiều chiều không thể suy ra phần tử tách biệt một chiều. Bởi vì một phần tử có nhiều yếu tố tách biệt một chiều chưa hẳn là tách biệt nhiều chiều. Ngược lại, một phần tử tách biệt nhiều chiều có thể chỉ có một thuộc tính là tách biệt một chiều.

Bài toán phát hiện phần tử tách biệt nhiều chiều là bài toán cơ bản nhất trong các hệ thống IDS dựa trên phát hiện bất thường. Với cách tiếp cận dựa trên xác suất, có nhiều nghiên cứu được đưa ra nhằm giải bài toán phát hiện phần tử tách biệt, người ta xây dựng các mô hình dữ liệu dựa trên phân bố ngẫu nhiên và xác định phần tử tách biệt thông qua mối tương quan với mô hình đó. Tuy nhiên khi số chiều của không gian mẫu tăng lên thì việc tính toán trở nên khó khăn và không chính xác.

Dựa trên kỹ thuật KPDL, vấn đề tìm kiếm phần tử tách biệt trong một tập dữ liệu được xử lý bằng nhiều cách khác nhau. Trên thực tế có nhiều thuật toán được sử dụng để tìm kiếm phần tử tách biệt, tuy nhiên có một thuật toán thường được sử dụng trong hệ thống phát hiện bất thường là thuật toán LOF. Thuật toán này được trình bày ở mục sau.

### b. Thuật toán LOF

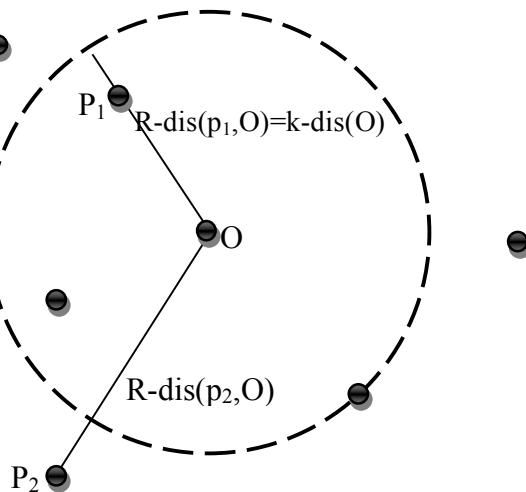
Thuật toán LOF (Local Outlier Factor) sử dụng hướng tiếp cận dựa trên mật độ được Breuning đưa ra trong [12]. Ý tưởng chính của phương pháp này là gán cho mỗi mẫu dữ liệu một cấp độ tách biệt. Cấp độ này còn được gọi là nhân tố tách biệt địa phương (Local Outlier Factor) của mẫu dữ liệu.

Như vậy đối với từng mẫu, mật độ phần tử lân cận đóng một vai trò then chốt. Lúc này, một mẫu không phải được phân loại là “tách biệt” hay “không tách biệt” mà được đánh giá là mức độ tách biệt như thế nào, tùy theo giá trị LOF của mẫu đó.

Ký hiệu  $k - dis(x)$  là khoảng cách đến phần tử lân cận thứ  $k$  của mẫu  $x$

Ký hiệu  $N_{k-dis}(x)$  là số lượng phần tử lân cận của  $x$  có khoảng cách tới  $x$  bé hơn  $k - dis(x)$

Khoảng cách tiếp cận trung bình của một mẫu  $x$  đối với một mẫu  $y$ , ký hiệu là  $R-dis(x,y)$  được tính như sau:  $R-dis(x,y)=\max(k-dis(x),d(x,y))$



Khoảng cách tiếp cận  $R-dis$

Chẳng hạn có 6 phần tử như trên,  $R\text{-dis}(p_1, O)$  và  $R\text{-dis}(p_2, O)$  được tính trong trường hợp  $k=3$ .

Theo Breuning [12], giá trị LOF của một phần tử  $x$  được tính như sau:

$$LOF = \left[ \frac{\sum_{y \in N_{MnPts}(x)} \frac{lrd_{MnPts}(y)}{lrd_{MnPts}(x)}}{|N_{MnPts}(x)|} \right]$$

Trong đó:

Hàm  $lrd(\cdot)$  chỉ *Mật độ tiếp cận địa phương* (*Local reachability density*) của một mẫu. Hàm  $lrd(\cdot)$  dựa trên tích nghịch đảo của  $R\text{-dis}(x, y)$  và dựa trên  $MnPts$  (số lượng mẫu tối thiểu) các phần tử lân cận của mẫu  $x$ .

Thuật toán tính LOF cho tất cả các mẫu dữ liệu được thực hiện qua các bước sau:

Bước 1: Đôi với mỗi mẫu  $x$  tính  $k\text{-dis}(x)$

Bước 2: Đôi với mỗi mẫu  $y$  tính  $R\text{-dis}(x, y)$

Bước 3: Tính hàm  $lrd(\cdot)$

Bước 4: Tính  $LOF(x)$

### c. Môđun lọc tin

Dữ liệu được thu thập từ nhiều nguồn khác nhau như Sensor, thiết bị mạng, từ SNMP MIB hay file log của các hệ thống. Do khối lượng dữ liệu rất lớn nên hệ thống không thể lưu trữ toàn bộ dữ liệu này. Hệ thống sẽ tiến hành quan sát theo dạng cửa sổ thời gian. Chẳng hạn như chỉ lưu trữ thông tin trong vòng 1 giờ trở lại. Độ dài cửa sổ quan sát cũng là một yếu tố mà người quản trị phải lựa chọn sao cho phù hợp với hệ thống mạng của mình. Nếu cửa sổ quá ngắn, hệ thống của sổ có thể bỏ lỡ nhiều tấn công dạng “chậm”. Ngược lại, trong

trường hợp cửa sổ quá dài thì hệ thống có thể sẽ không đảm bảo tốc độ, không thích hợp trong môi trường thời gian thực.

Các bộ dữ liệu thông thường được lưu trên file ở dạng bản ghi. Hệ thống sẽ truy cập các file này để lấy thông tin. Môđun lọc tin có chức năng loại bỏ những thông tin thừa, các lưu lượng mà hệ thống biết chắc không có tác dụng. Những thông tin có ích cho hệ thống chỉ chiếm khoảng 20% tổng số thông tin mà công cụ bắt gói tin đưa về.

#### d. Môđun trích xuất dữ liệu

Dữ liệu sau khi qua module lọc sẽ được tiến hành trích xuất các yếu tố quan sát. Mỗi một thuật toán phát hiện bất thường sẽ có một tập các thông số quan sát riêng. Thông thường đối với các gói tin mạng, thông tin qua trọng chủ yếu nằm ở phần Header của gói tin. Sau đây là một số thông số mà module trích xuất thông tin có thể sử dụng đến:

Header	Thông tin trích xuất
Ethernet header	Packet size Source address Destination address Protocol
IP header	Source address Destination address Header length TOS Packet size IP Fragment ID

	IP Flag & Pointer TTL Checksum
TCP header	Source port, Destination port Sequency & ACK Number Header length Window size Checksum
UDP header	Source port, Destination port Checksum Length
ICMP	Type & Code Checksum

#### e. Môđun phát hiện phân tử tách biệt

Trong module này thông thường người ta sử dụng thuật toán Phát hiện phân tử tách biệt. Tùy thuộc vào sự phân bố trên Bộ dữ liệu đầu vào mà thuật toán này hay thuật toán khác có được kết quả xử lý tốt hơn. Các kết quả thử nghiệm cho thấy đối với tính chất phân bố dữ liệu mạng, thuật toán LOF có tỷ lệ phát hiện tấn công cao và tỷ lệ cảnh báo thấp hơn so với các thuật toán khác.

#### f. Môđun tổng hợp

Trong một hệ thống mạng lớn có nhiều nút mạng, số lượng kết nối cần giám sát là rất lớn. Chẳng hạn trong 10 phút, có thể có đến hàng triệu kết nối được hình thành trong hệ thống mạng. Nếu 0,1% tổng số lượng các kết nối được đánh giá là có dấu hiệu bất thường, thì trong 10 phút có hàng trăm cảnh báo được phát ra, điều này gây khó khăn cho khả năng giám sát và nhận định của người quản trị. Do đó cần thiết phải có một biện pháp nhằm tổng hợp các kết nối được đánh dấu là bất thường để rút gọn dữ liệu đầu ra, trong khi vẫn phản ánh chính xác tình trạng bất thường.

Ngoài ra, sau khi các dạng tấn công mới được phát hiện, cần thiết phải bổ sung các mẫu của dạng tấn công này cho hệ thống phát hiện xâm nhập dựa trên dấu hiệu. Các mẫu này phải là các tập luật ở dạng rút gọn, có thể phản ánh đúng được các cuộc tấn công mới và thuận tiện trong việc so sánh kiểm tra trong tương lai.

Để đáp ứng các yêu cầu đó, người ta sử dụng kỹ thuật tổng hợp trong KPDL nhằm rút gọn các cảnh báo và tập mẫu. Sau đây là một ví dụ về cách tổng hợp cảnh báo. Một bảng gồm 10 cảnh báo tương đối giống nhau sẽ được rút gọn thành một cảnh báo.

SrcIP	Start time	Dest IP	Dest port	Number of bytes
X.Y.Z.95	11.07.20	A.B.C.223	139	192
X.Y.Z.95	11.13.56	A.B.C.219	139	195
X.Y.Z.95	11.14.29	A.B.C.217	139	180
X.Y.Z.95	11.14.30	A.B.C.255	139	199
X.Y.Z.95	11.14.32	A.B.C.254	139	186
X.Y.Z.95	11.14.35	A.B.C.253	139	177
X.Y.Z.95	11.14.36	A.B.C.252	139	172
X.Y.Z.95	11.14.38	A.B.C.251	139	192
X.Y.Z.95	11.14.41	A.B.C.250	139	195

Summarization  
→ SrcIP=X.Y.Z.95,

*Ví dụ về tổng hợp luật*

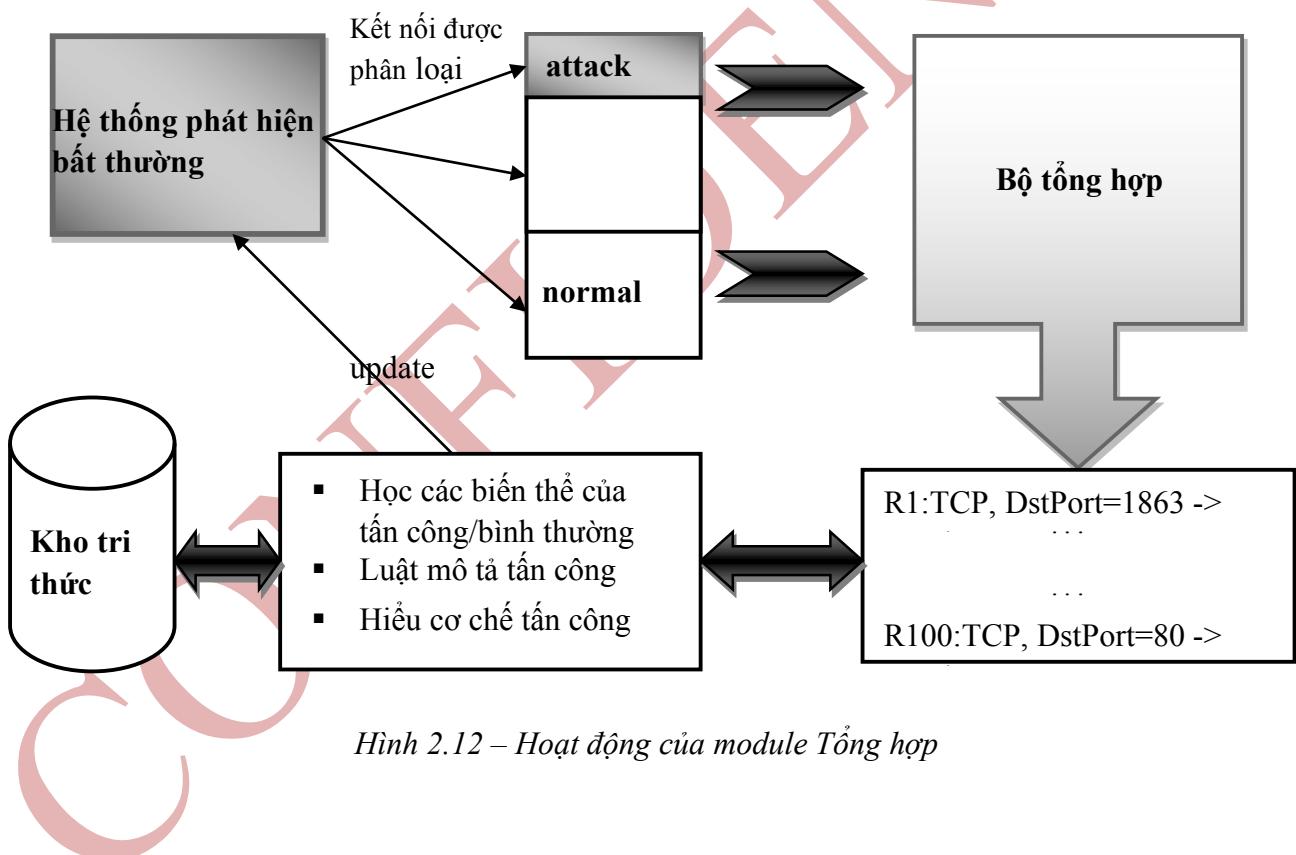
Ý tưởng của module này tương tự quá trình ~~lộ~~ tóm tắt văn bản. Có thể sử dụng các thuật toán tóm tắt văn bản để thực hiện chức năng module này. Ở đây trình bày một thuật toán tổng hợp dựa trên 2 yếu tố là *độ nén* và *tỉ lệ mất tin*.

Độ nén nhấn mạnh đến tính rút gọn của dữ liệu, *tỷ lệ mất tin* nhấn mạnh sự mất mát thông tin sau khi áp dụng quá trình tổng hợp dữ liệu. Trong cùng một thuật toán thì nếu ta tăng *độ nén*, *tỷ lệ mất tin* cũng tăng theo. Do vậy cần phải có sự cân đối hợp lý giữa 2 yếu tố này. Bằng cách sử dụng hàm định lượng:

$$S = k * (\text{độ nén}) - (\text{tỷ lệ mất tin})$$

Trong đó, k là hằng số do người dùng chọn, nó là biến điều chỉnh mức độ quan tâm giữa tỷ lệ nén và tỷ lệ mất gói tin.

Dữ liệu đầu vào của Module Tổng hợp là các kết nối được gán chỉ số bất thường từ Module Phát hiện PTTB, đầu ra là các mẫu rút gọn mô tả cuộc tấn công.



Hình 2.12 – Hoạt động của module Tống hợp

Module tổng hợp sử dụng các thuật toán heuristic để lựa chọn cách rút gọn tập cảnh báo sao cho phù hợp. Một thuật toán heuristic giải quyết vấn đề này thường trải qua những bước sau:

Bước 1: Dựa trên tập cảnh báo từ module Phát hiện tách biệt, tiến hành tính toán các tần suất xuất hiện của các tập yếu tố quan sát

Bước 2: Đưa ra một danh sách các ứng cử viên rút gọn

Bước 3: Tính toán vét cạn đối với từng trường hợp. Mỗi trường hợp sẽ tính hàm định lượng  $S = k^*(\text{độ nén}) - (\text{tỷ lệ mất tin})$ .

Bước 4: Chọn ra một ứng cử viên có hàm  $S$  lớn nhất. Thực hiện rút gọn theo ứng cử viên này. Loại bỏ các cảnh báo đã nằm trong quá trình rút gọn này. Tiếp tục với ứng cử viên khác cho đến khi toàn bộ danh sách cảnh báo được rút gọn.

*Ví dụ ta có các cảnh báo sau:*

	src IP	sPort	dst IP	dPort	proto	flags	packets	bytes
--	--------	-------	--------	-------	-------	-------	---------	-------

T1	12.190.84.122	32178	100.10.20.4	80	tcp	—APRS-	[2,20]	[504,1200]
T2	88.34.224.2	51989	100.10.20.4	80	tcp	—APRS-	[2,20]	[220,500]
T3	12.190.19.23	2234	100.10.20.4	80	tcp	—APRS-	[2,20]	[220,500]
T4	98.198.66.23	27643	100.10.20.4	80	tcp	—APRS-	[2,20]	[42,200]
T5	192.168.22.4	5002	100.10.20.3	21	tcp	—A-RSF	[40,68]	[42,200]
T6	192.168.22.4	5001	100.10.20.3	21	tcp	—A-RSF	[40,68]	[220,500]
T7	67.118.25.23	44532	100.10.20.3	21	tcp	—A-RSF	[2,20]	[42,200]

T8	192.168.22.4	2765	100.10.20.4	113	tcp	—APRS-		[504,1200]
----	--------------	------	-------------	-----	-----	--------	--	------------

Tập ứng cử viên có thể là các yếu tố quan sát hoặc bộ yếu tố quan sát có tần suất xuất hiện cao  
như: {[srcIP=192.168.22.4],[dstIP=100.10.20.4;pro=tcp;  
flags=—APRS,packets=2,20],[dPort=80],[srcIP=192.168.22.4;dstIP=100.10.20.3],[dstIP=100.10.20.4;dPort=80] . . .}

Lần lượt thực hiện thuật toán rút gọn, các cảnh báo sau sẽ chỉ còn 3 dòng như sau:

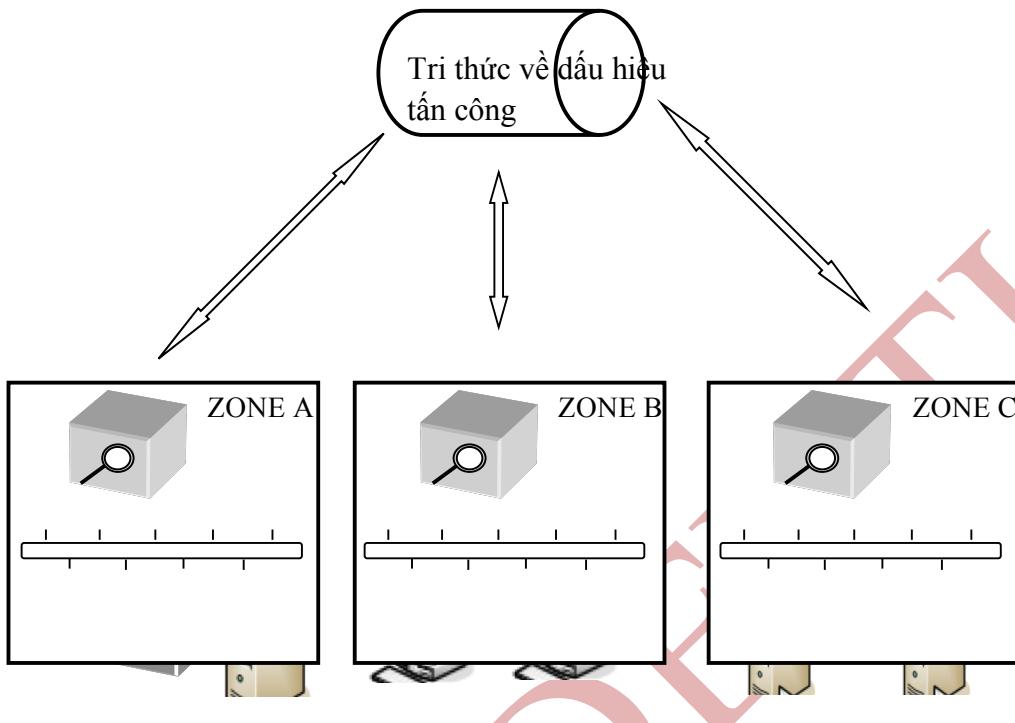
	src IP	sPort	dst IP	dPort	pro	flags	packets	bytes
--	--------	-------	--------	-------	-----	-------	---------	-------

S1	*.*.*.*	***	100.10.20.4	80	tcp	—APRS-	[2,20]	***
S2	*.*.*.*	***	100.10.20.3	21	tcp	—A-RSF	***	***
S3	192.168.22.4	2765	100.10.20.4	113	tcp	—APRS-	[2,20]	[504,1200]

Hạn chế của nhiều hệ thống phát hiện bất thường trước đây là không có quá trình học phản hồi từ chuyên gia, Nghĩa là các cảnh báo sai sẽ tiếp tục được đưa ra ở những lần sau. Đối với hệ thống sử dụng KPDL, sau khi hình thành các cảnh báo rút gọn, module tổng hợp chuyển cho các chuyên gia xem xét và quyết định những cảnh báo nào là cảnh báo đúng và có tần công thực sự. Các tri thức này sẽ được cập nhật vào Bộ dữ liệu của hệ thống nhằm phát hiện các tần công đã biết ở những lần sau. Sử dụng phản hồi của chuyên gia là một hướng mới giúp cho hệ thống liên tục được cập nhật và ổn định hơn khi phát hiện tần công.

Các hệ thống IDS được đặt ở các vùng mạng khác nhau và giám sát lưu thông vào ra ở các vùng mạng đó. Mỗi hệ thống hoạt động và học tập tri thức một cách độc lập về tần công ở

từng vùng. Để nâng cao khả năng phối hợp giữa các hệ thống IDS, cần thiết nên có một bộ tri thức chung và sự phối hợp giữa các hệ thống IDS.



## 4.2 Phần mềm độc hại

### 4.2.1 Virus

#### a. Định nghĩa Virus.

Trong khoa học máy tính, virus máy tính (thường được người sử dụng gọi tắt là virus) là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng lây nhiễm khác (file, ổ đĩa, máy tính ..).

Trước đây, virus thường được viết bởi một số người am hiểu về lập trình muốn chứng tỏ khả năng của mình nên thường virus có các hành động như: cho một chương trình không hoạt động đúng, xóa dữ liệu, làm hỏng ổ cứng,... hoặc gây ra những trò đùa khó chịu.

Những virus mới được viết trong thời gian gần đây không còn thực hiện các trò đùa hay sự phá hoại đối máy tính của nạn nhân bị lây nhiễm nữa, mà đa phần hướng đến việc lây cắp các thông tin cá nhân nhạy cảm (các mã số thẻ tín dụng) mở cửa sau cho tin tặc đột nhập chiếm quyền điều khiển hoặc các hành động khác nhằm có lợi cho người phát tán virus.

Chiếm trên 90% số virus đã được phát hiện là nhắm vào hệ thống sử dụng hệ điều hành họ Windows chỉ đơn giản bởi hệ điều hành này được sử dụng nhiều nhất trên thế giới. Do tính thông dụng của Windows nên các tin tặc thường tập trung hướng vào chúng nhiều hơn là các hệ điều hành khác. (Cũng có quan điểm cho rằng Windows có tính bảo mật không tốt bằng các hệ điều hành khác (như Linux) nên có nhiều virus hơn, tuy nhiên nếu các hệ điều hành khác cũng thông dụng như Windows hoặc thị phần các hệ điều hành ngang bằng nhau thì cũng lượng virus xuất hiện có lẽ cũng tương đương nhau).

### b. Phân loại Virus.

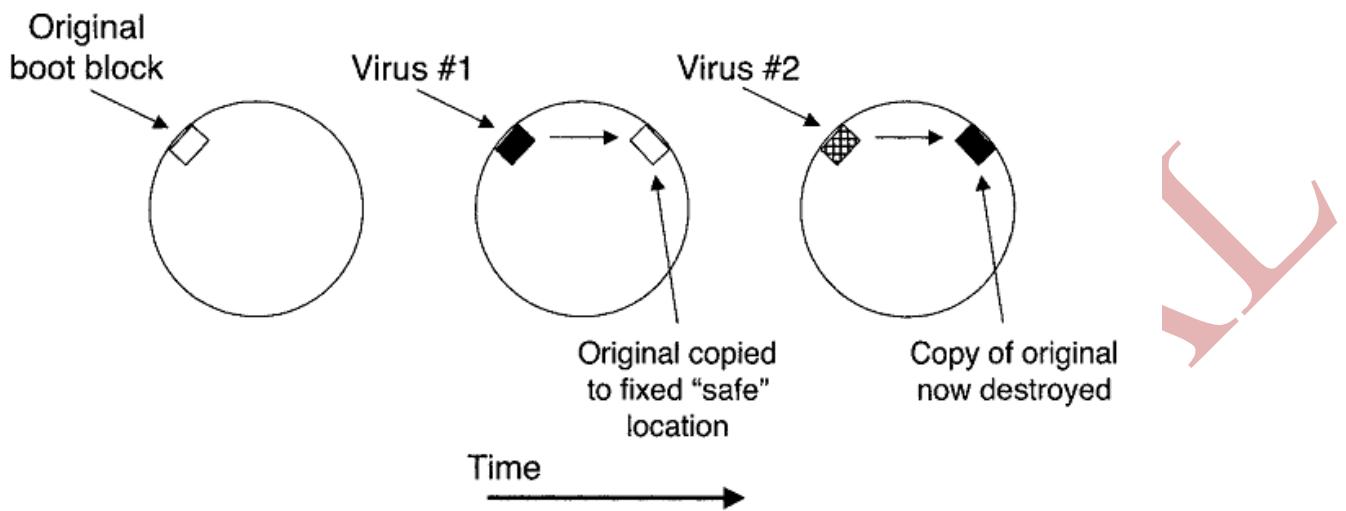
Một trong những phương pháp thường thấy để phân loại virus là theo cách lây nhiễm của chúng. Phương pháp này chia virus ra làm 3 loại: Virus lây nhiễm boot-sector, virus lây nhiễm các file thực thi, và virus lây nhiễm các file dữ liệu.

### c. Virus lây nhiễm boot-sector

Quá trình lây nhiễm boot cơ bản qua các bước:

- Bước 1: Khởi động.
- Bước 2: Chạy các tập lệnh trong ROM, thực hiện quá trình self-test, nhận dạng thiết bị và khởi tạo. Thiết bị khởi động được xác định, và khôi khởi động được đọc từ thiết bị này, thông thường khôi khởi động là tập hợp các khôi đầu tiên của thiết bị khởi động. Một khi khôi khởi động được đọc, quyền điều khiển được trao cho khôi này. Bước này gọi là primary bootsector

## Viruses



- Bước 3: Trong bước này, tập hợp các chương trình kiểm soát file hệ thống thiết bị khởi động được trao quyền và thực thi. Bước này gọi là secondary boot
- Bước 4: Hệ điều hành được tải lên bởi các chương trình trên.

Năm 1986: Virus "the Brain", virus cho máy tính cá nhân (PC) đầu tiên, được tạo ra tại Pakistan bởi Basit và Amjad. Chương trình này nằm trong phần khởi động (boot sector) của một đĩa mềm 360Kb và nó sẽ lây nhiễm tất cả các ổ đĩa mềm. Đây là loại "stealth virus" đầu tiên.

### Virus lây nhiễm file thực thi

Nguyên tắc của F-virus là gắn lén vào file thực thi (dạng .COM và .EXE) một đoạn mã ở phần đầu hoặc cuối của cấu trúc file để mỗi lần file thực hiện, đoạn mã này sẽ được kích hoạt, thường trú trong vùng nhớ, không chép các tác vụ truy xuất file, dò tìm các file thực thi sạch khác để tự gắn chúng vào. Ưu điểm của F-virus là dễ dàng được kích hoạt (do tần suất chạy chương trình COM, EXE của hệ thống rất cao). Nhược điểm của chúng là chỉ lây trên một hệ điều hành xác định.

Tháng 12 năm 1986, virus cho DOS được khám phá ra là virus "VirDem". Nó có khả năng tự chép mã của mình vào các tệp tự thi hành (executable file) và phá hoại các máy tính VAX/VMS.

Năm 1987: Virus đầu tiên tấn công vào command.com là virus "Lehigh".

Năm 1988: Virus Jerusalem tấn công đồng loạt các đại học và các công ty trong các quốc gia vào ngày thứ Sáu 13. Đây là loại virus hoạt động theo đồng hồ của máy tính (giống bom nổ chậm cài hàng loạt cho cùng một thời điểm).

Tháng 11 cùng năm, Robert Morris, 22 tuổi, chế ra worm chiếm cứ các máy tính của ARPANET, làm liệt khoảng 6.000 máy. Morris bị phạt tù 3 năm và 10.000 dollar.

### Virus lây nhiễm file dữ liệu

Lợi dụng như câu trao đổi văn bản, thư từ, công văn, hợp đồng ... trong thời đại bùng nổ thông tin, kẻ thiết kế nên virus Concept (thủy tổ của họ virus macro) chọn ngôn ngữ macro của Microsoft Word làm phương tiện lây lan trên môi trường Winword. Khi bạn mở một tài liệu \*.DOC bị nhiễm virus thì từ văn bản nhiễm macro virus sẽ được đưa vào file NORMAL.DOT, rồi từ đây, chúng tự chèn vào các văn bản sạch khác. Dạng thứ hai của virus macro là lây vào bảng tính của Microsoft Excel, ít phổ biến hơn dạng thứ nhất.

Virus macro độc ở chỗ nó làm mọi người nghi ngờ lẫn nhau. Hãy tưởng tượng bạn nhận được file \*.DOC từ người bạn thân, chắc chắn bạn sẽ không ngần ngại mở ra xem. Mặc dù người gởi không có tình hại bạn, nhưng biết đâu có ẩn chứa virus, và đúng lúc bạn chờ Word in ra màn hình nội dung bức thư thì toàn bộ đĩa cứng của bạn đã bị xóa trống. Đó là độc chiêu mà macro virus NTTNTA sẽ xóa đĩa cứng khi số lần mở các file nhiễm là 20.

Năm 1995: Virus văn bản (macro virus) đầu tiên xuất hiện trong các mã macro trong các tệp của Word và lan truyền qua rất nhiều máy. Loại virus này có thể làm hư hệ điều hành chủ. Macro virus là loại virus viết ra bằng ngôn ngữ lập trình Visual Basic cho các ứng dụng (VBA) và tùy theo khả năng, có thể lan nhiễm trong các ứng dụng văn phòng của Microsoft như Word, Excel, PowerPoint, OutLook,... Loại macro này, nổi tiếng có virus Baza và virus Laroux, xuất hiện năm 1996, có thể nằm trong cả Word hay Excel. Sau này, virus Melissa, năm 1997, tấn công hơn 1 triệu máy, lan truyền bởi một tệp đính kèm kiểu Word bằng cách đọc và gửi đến các địa chỉ của Outlook trong các máy đã bị nhiễm virus. Virus Tristate, năm 1999, có thể nằm trong các tệp Word, Excel và Power Point.

Năm 2000: Virus Love Bug, còn có tên ILOVEYOU, đánh lừa tính hiếu kì của mọi người. Đây là một loại macro virus. Đặc điểm là nó dùng đuôi tập tin dạng "ILOVEYOU.txt.exe". Lợi dụng điểm yếu của Outlook thời bấy giờ: theo mặc định sẵn, đuôi dạng .exe sẽ tự động bị dấu đi. Ngoài ra, virus này còn có một đặc tính mới của spyware: nó tìm cách đọc tên và mã nhập của máy chủ và gửi về kẻ tạo ra virus. Tác giả của loại virus này là một sinh viên người Philippines.

#### 4.2.2 Anti-Virus

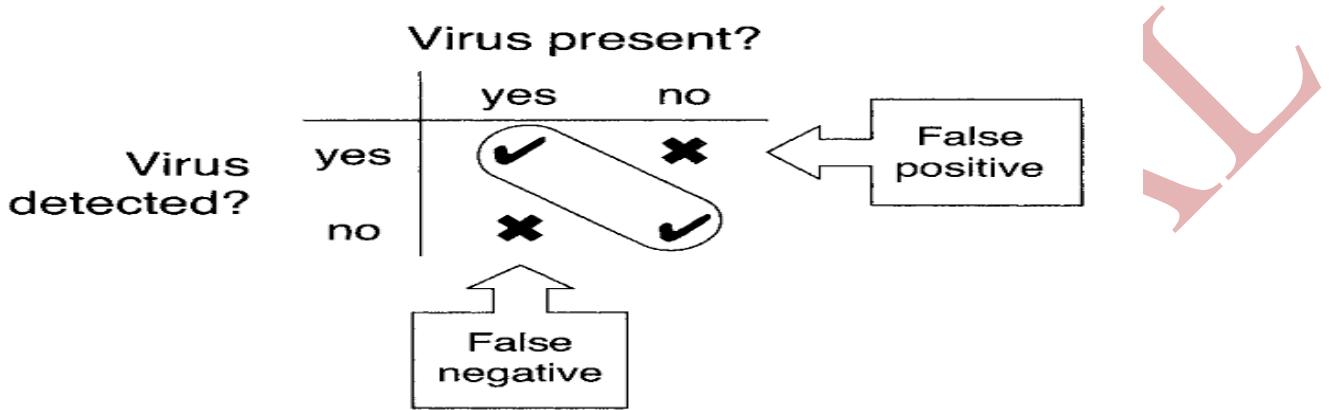
Các phần mềm phòng chống virus thực hiện 3 tác vụ chính:

- **Sự nhận biết virus:** Là phát hiện có hoặc không mã của một loại virus hay không mà, cách thức cơ bản nhất để phát hiện virus, giá trị trả lại ở dạng Boolean: YES – có nghĩa là trong mã này có virus; NO - mã này không bị nhiễm bệnh. Cuối cùng, phát hiện là một mất. Tuy vậy đây cũng không phải là một cách thức thực sự hiệu quả để phát hiện được virus bởi suy cho cùng cách xuất hiện hoặc hành vi của virus là khó có thể dự đoán được. Một người với kỹ thuật có thể viết nên một virus mà các chương trình diệt virus không thể phát hiện được. (Lưu ý rằng: virus này sau đó có thể được phát hiện bởi các chương trình chống virus với quá trình cập nhật các virus mới. Tuy nhiên tác giả của virus cũng có thể tạo ra một phiên bản mới của virus. Quá trình phát hiện và phát triển virus này diễn ra một cách liên tục).

Một câu hỏi được đặt ra là : Có nên một virus luôn được phát hiện, ngay cả khi nó không thể chạy? Câu trả lời là :Có. Bởi ngay cả khi một virus là không hoạt động trên một hệ thống, nó vẫn còn hữu ích để phát hiện nó để vi rút không ảnh hưởng đến hệ thống khác. Trong các trường hợp dù virus không chạy trên bất kỳ hệ thống nào thì việc tìm một virus có thể giúp chỉ ra một số lỗ hổng bảo mật tiềm ẩn, và do đó nó là hữu ích để phát hiện những virus trên.

- **Sự xác định virus:** Một khi virus được phát hiện, nó cần được xác định xem đó là loại virus gì? Quá trình xác định có thể là riêng biệt với phát hiện, hoặc nó có thể được thực hiện như một phần của phương pháp phát hiện virus được sử dụng.

- **Sự ngăn nhiễm hoặc loại bỏ virus:** Là quá trình loại bỏ virus được phát hiện, đôi khi quá trình này được gọi là làm sạch. Thông thường một virus sẽ cần phải được xác định chính xác trước khi thực hiện làm sạch nhằm có biện pháp hiệu quả nhất.



Quá trình phát hiện và loại bỏ có thể được thực hiện bằng việc sử dụng các phương pháp chung có khả năng nhận biết cả các virus đã biết và chưa biết. Với các virus đã biết thường sử dụng các phương pháp cụ thể để nâng cao hiệu quả phát hiện và loại bỏ (Lưu ý: Các phương pháp cụ thể dành cho các loại virus đã biết cũng có thể phát hiện được các biến thể chưa biết của loại virus đó.)

Trong 3 quá trình trên thì quá trình phát hiện được coi là quan trọng nhất, bởi vì quá trình xác định và loại bỏ cần quá trình phát hiện như là một điều kiện tiên quyết. Ngoài ra, phát hiện sớm (tức là, trước khi lây nhiễm xảy ra) hoàn toàn làm giảm bớt sự cần thiết cho các nhiệm vụ khác. Có năm kết quả có thể phát hiện. Hình trên cho thấy bốn trong số đó. Phát hiện virus một cách chính xác trong hai trường hợp: không có virus tồn tại quá trình phát hiện đưa ra kết quả là không tồn tại virus và ngược lại đưa ra kết quả là tồn tại virus khi thực sự có virus tồn tại. Phát hiện được coi là false positive khi phần mềm antivirus báo có virus nhưng trên thực tế virus lại không tồn tại. Và phát hiện được coi là false negative khi quá trình phát hiện không thể phát hiện ra virus mặc dù trên thực tế là có tồn tại. Kết quả thứ năm là ghost positives khi virus thực chất đã không còn xong quá trình phát hiện vẫn báo tồn tại virus bởi do quá trình loại bỏ trước đó chưa triệt để và vẫn còn tồn tại tàn dư của virus đủ để quá trình phát hiện báo rằng vẫn còn tồn tại virus. Có hai phương

pháp phát hiện là phát hiện tĩnh và phát hiện động, phụ thuộc vào có hoặc không mã virus đang chạy khi việc phát hiện xảy ra.

## **Phòng chống Virus.**

Có một câu nói vui rằng Để không bị lây nhiễm virus thì ngắt kết nối khỏi mạng, không sử dụng ổ mềm, ổ USB hoặc copy bất kỳ file nào vào máy tính. Nhưng nghiêm túc ra thì điều này có vẻ đúng khi mà hiện nay sự tăng trưởng số lượng virus hàng năm trên thế giới rất lớn.

Không thể khẳng định chắc chắn bảo vệ an toàn 100% cho máy tính trước hiểm họa virus và các phần mềm hiểm độc, nhưng chúng ta có thể hạn chế đến tối đa có thể và có các biện pháp bảo vệ dữ liệu của mình.

### **a. Sử dụng phần mềm diệt virus**

Bảo vệ bằng cách trang bị thêm một phần mềm diệt virus có khả năng nhận biết nhiều loại virus máy tính và liên tục cập nhật dữ liệu để phần mềm đó luôn nhận biết được các virus mới.

Trên thị trường hiện có rất nhiều phần mềm diệt virus. Một số hãng nổi tiếng viết các phần mềm virus được nhiều người sử dụng có thể kể đến là: McAfee, Symantec, Kaspersky

### **b. Sử dụng tường lửa**

Tường lửa (Firewall) không phải một cái gì đó quá xa vời hoặc chỉ dành cho các nhà cung cấp dịch vụ internet (ISP) mà mỗi máy tính cá nhân cũng cần phải sử dụng tường lửa để bảo vệ trước virus và các phần mềm độc hại. Khi sử dụng tường lửa, các thông tin vào và ra đối với máy tính được kiểm soát một cách vô thức hoặc có chủ ý. Nếu một phần mềm độc hại đã được cài vào máy tính có hành động kết nối ra Internet thì tường lửa có thể cảnh báo giúp người sử dụng loại bỏ hoặc vô hiệu hóa chúng. Tường lửa giúp ngăn chặn các kết nối đến không mong muốn để giảm nguy cơ bị kiểm soát máy tính ngoài ý muốn hoặc cài đặt vào các chương trình độc hại hay virus máy tính.

Sử dụng tường lửa bằng phần cứng nếu người sử dụng kết nối với mạng Internet thông qua một modem có chức năng này. Thông thường ở chế độ mặc định của nhà sản xuất thì chức năng "tường lửa" bị tắt, người sử dụng có thể truy cập vào modem để cho phép hiệu lực (bật). Sử dụng tường lửa bằng phần cứng không phải tuyệt đối an toàn bởi chúng thường chỉ ngăn chặn kết nối đến trái phép, do đó kết hợp sử dụng tường lửa bằng các phần mềm.

Sử dụng tường lửa bằng phần mềm: Ngay các hệ điều hành họ Windows ngày nay đã được tích hợp sẵn tính năng tường lửa bằng phần mềm, tuy nhiên thông thường các phần mềm của hãng thứ ba có thể làm việc tốt hơn và tích hợp nhiều công cụ hơn so với tường lửa phần mềm sẵn có của Windows. Ví dụ bộ phần mềm ZoneAlarm Security Suite của hãng ZoneLab là một bộ công cụ bảo vệ hữu hiệu trước virus, các phần mềm độc hại, chống spam, và tường lửa.

### c. Cập nhật các bản sửa lỗi của hệ điều hành

Hệ điều hành Windows (chiếm đa số) luôn luôn bị phát hiện các lỗi bảo mật chính bởi sự thông dụng của nó, tin tặc có thể lợi dụng các lỗi bảo mật để chiếm quyền điều khiển hoặc phát tán virus và các phần mềm độc hại. Người sử dụng luôn cần cập nhật các bản vá lỗi của Windows thông qua trang web Microsoft Update (cho việc nâng cấp tất cả các phần mềm của hãng Microsoft) hoặc Windows Update (chỉ cập nhật riêng cho Windows). Cách tốt nhất hãy đặt chế độ nâng cấp (sửa chữa) tự động (Automatic Updates) của Windows. Tính năng này chỉ hỗ trợ đối với các bản Windows mà Microsoft nhận thấy rằng chúng hợp pháp.

### d. Vận dụng kinh nghiệm sử dụng máy tính

Cho dù sử dụng tất cả các phần mềm và phương thức trên nhưng máy tính vẫn có khả năng bị lây nhiễm virus và các phần mềm độc hại bởi mẫu virus mới chưa được cập nhật kịp thời đối với phần mềm diệt virus. Người sử dụng máy tính cần sử dụng triệt để các chức năng, ứng dụng sẵn có trong hệ điều hành và các kinh nghiệm khác để bảo vệ cho hệ điều hành và dữ liệu của mình. Một số kinh nghiệm tham khảo như sau:

Phát hiện sự hoạt động khác thường của máy tính: Đa phần người sử dụng máy tính không có thói quen cài đặt, gỡ bỏ phần mềm hoặc thường xuyên làm hệ điều hành thay đổi - có nghĩa là một sự sử dụng ổn định - sẽ nhận biết được sự thay đổi khác thường của máy tính. Ví dụ đơn giản: Nhận thấy sự hoạt động chậm chạp của máy tính, nhận thấy các kết nối ra ngoài khác thường thông qua tường lửa của hệ điều hành hoặc của hãng thứ ba (thông qua các thông báo hỏi sự cho phép truy cập ra ngoài hoặc sự hoạt động khác của tường lửa). Mọi sự hoạt động khác thường này nếu không phải do phần cứng gây ra thì cần nghi ngờ sự xuất hiện của virus. Ngay khi có nghi ngờ, cần kiểm tra bằng cách cập nhật dữ liệu mới nhất cho phần mềm diệt virus hoặc thử sử dụng một phần mềm diệt virus khác để quét toàn hệ thống.

Kiểm soát các ứng dụng đang hoạt động: Kiểm soát sự hoạt động của các phần mềm trong hệ thống thông qua Task Manager hoặc các phần mềm của hãng thứ ba (chẳng hạn: ProcessViewer) để biết một phiên làm việc bình thường hệ thống thường nạp các ứng dụng nào, chúng chiếm lượng bộ nhớ bao nhiêu, chiếm CPU bao nhiêu, tên file hoạt động là gì...ngay khi có điều bất thường của hệ thống (dù chưa có biểu hiện của sự nhiễm virus) cũng có thể có sự nghi ngờ và có hành động phòng ngừa hợp lý. Tuy nhiên cách này đòi hỏi một sự am hiểu nhất định của người sử dụng.

Loại bỏ một số tính năng của hệ điều hành có thể tạo điều kiện cho sự lây nhiễm virus: Theo mặc định Windows thường cho phép các tính năng autorun giúp người sử dụng thuận tiện cho việc tự động cài đặt phần mềm khi đưa đĩa CD hoặc đĩa USB vào hệ thống. Chính các tính năng này được một số loại virus lợi dụng để lây nhiễm ngay khi vừa cắm ổ USB hoặc đưa đĩa CD phần mềm vào hệ thống (một vài loại virus lan truyền rất nhanh trong thời gian gần đây thông qua các ổ USB bằng cách tạo các file autorun.ini trên ổ USB để tự chạy các virus ngay khi cắm ổ USB vào máy tính). Cần loại bỏ tính năng này bằng các phần mềm của hãng thứ ba như TWEAKUI hoặc sửa đổi trong Registry.

#### e. Bảo vệ dữ liệu máy tính

Nếu như không chắc chắn 100% rằng có thể không bị lây nhiễm virus máy tính và các phần mềm hiểm độc khác thì bạn nên tự bảo vệ sự toàn vẹn của dữ liệu của mình trước

khi dữ liệu bị hư hỏng do virus (hoặc ngay cả các nguy cơ tiềm tàng khác như sự hư hỏng của các thiết bị lưu trữ dữ liệu của máy tính). Trong phạm vi về bài viết về virus máy tính, bạn có thể tham khảo các ý tưởng chính như sau:

Sao lưu dữ liệu theo chu kỳ là biện pháp đúng đắn nhất hiện nay để bảo vệ dữ liệu. Bạn có thể thường xuyên sao lưu dữ liệu theo chu kỳ đến một nơi an toàn như: các thiết bị nhớ mở rộng (ổ USB, ổ cứng di động, ghi ra đĩa quang...), hình thức này có thể thực hiện theo chu kỳ hàng tuần hoặc khác hơn tùy theo mức độ cập nhật, thay đổi của dữ liệu của bạn.

Tạo các dữ liệu phục hồi cho toàn hệ thống không dùng lại các tiện ích sẵn có của hệ điều hành (ví dụ System Restore của Windows Me, XP...) mà có thể cần đến các phần mềm của hãng thứ ba, ví dụ bạn có thể tạo các bản sao lưu hệ thống bằng các phần mềm ghost, các phần mềm tạo ảnh ổ đĩa hoặc phân vùng khác.

Thực chất các hành động trên không chắc chắn là các dữ liệu được sao lưu không bị lây nhiễm virus, nhưng nếu có virus thì các phiên bản cập nhật mới hơn của phần mềm diệt virus trong tương lai có thể loại bỏ được chúng.

#### 4.2.3 Worm

Worm hay sâu máy tính là một chương trình máy tính có khả năng tự nhân bản giống như virus máy tính. Trong khi virus máy tính bám vào và trở thành một phần của mã máy tính để có thể thi hành thì sâu máy tính là một chương trình độc lập không nhất thiết phải là một phần của một chương trình máy tính khác để có thể lây nhiễm. Sâu máy tính thường được thiết kế để khai thác khả năng truyền thông tin có trên những máy tính có các đặc điểm chung - cùng hệ điều hành hoặc cùng chạy một phần mềm mạng - và được nối mạng với nhau.

Sâu máy tính thường mang theo phần mềm gián điệp để mở cửa hậu máy tính trên các máy tính bị nhiễm (giống như Sobig và Mydoom). Các máy tính bị nhiễm được sử dụng bởi những người gửi thư rác hoặc giả danh địa chỉ trang web. Các cửa hậu cũng có thể được

các sâu máy tính khác khai thác như Doomjuice - phát tán bằng cửa hậu được mở bởi Mydoom.

Sâu máy tính lan truyền qua mạng hay qua các thiết bị lưu trữ di động như ổ USB

Sâu Morris là sâu máy tính đầu tiên được phát tán qua Internet; nó cũng là con sâu đầu tiên thu hút được sự chú ý đáng kể của các phương tiện thông tin đại chúng. Tác giả của nó là Robert Tappan Morris, một sinh viên tại Đại học Cornell. Sâu Morris được thả lên mạng vào ngày 2 tháng 11 năm 1988 từ học viện MIT, nó được phát tán từ MIT để che giấu thực tế là con sâu đã được bắt nguồn từ Cornell. (Tình cờ, Robert Tappan Morris hiện là một giáo sư tại MIT).

Theo tác giả, sâu Morris không được viết với mục đích gây thiệt hại mà chỉ để đo kích thước của Internet. Tuy nhiên, một hậu quả ngoài ý muốn đã làm cho nó trở nên gây hại: một máy tính có thể bị nhiễm nhiều lần và mỗi một tiến trình bổ sung sẽ góp phần làm chậm máy đến mức không thể sử dụng được. Sâu Morris hoạt động bằng cách lợi dụng một số điểm yếu đã biết trong các chương trình sendmail, Finger, rsh/rexec và các mật khẩu yếu trong Unix. Thân chương trình chính của sâu Morris chỉ có thể nhiễm các máy VAX của DEC đang chạy hệ điều hành BSD 4 và Sun 3. Một thành phần "móc" (grappling hook) khả chuyển viết bằng C theo cơ chế tràn bộ đệm đã được sử dụng để chở thân chương trình chính, và thành phần móc có thể chạy trên các hệ thống khác, sinh tài làm chậm hệ thống và biến hệ thống thành nạn nhân.

Sai lầm nghiêm trọng đã biến con sâu từ chỗ một thí nghiệm trí thức có tiềm năng vô hại thành một tấn công từ chối dịch vụ đầy phá hoại là ở tại cơ chế lây lan. Con sâu xác định xem có xâm nhập một máy tính mới hay không bằng cách hỏi xem hiện đã có một bản sao nào đang chạy hay chưa. Nhưng nếu chỉ làm điều này thì việc xóa bỏ nó lại quá dễ dàng, bất cứ ai cũng chỉ phải chạy một tiến trình trả lời rằng "có" khi được hỏi xem đã có bản sao nào chưa, và con sâu sẽ tránh. Để tránh chuyện này, Morris thiết kế để con sâu tự nhân đôi với xác suất 40%, bất kể kết quả của việc kiểm tra lây nhiễm là gì. Thực tế cho thấy tỷ lệ nhân đôi này là quá cao và con sâu lây lan nhanh chóng, làm nhiễm một số máy tính nhiều lần.

Người ta thống kê rằng có khoảng 6.000 máy tính chạy Unix đã bị nhiễm sâu Morris. Paul Graham đã nói rằng "Tôi đã chứng kiến người ta xào xáo ra con số này, công thức nấu ăn như sau: ai đó đoán rằng có khoảng 60.000 máy tính nối với Internet, và con sâu có thể đã nhiễm 10% trong số đó.". Mỹ đã ước tính thiệt hại vào khoảng từ 10 đến 100 triệu đô la.

Robert Morris đã bị xử và buộc tội vi phạm Điều luật năm 1986 về lạm dụng và gian lận máy tính (Computer Fraud and Abuse Act). Sau khi chống án, anh ta bị phạt 3 năm án treo, 400 giờ lao động công ích và khoản tiền phạt 10.050 đô la Mỹ.

Sâu Morris đôi khi được gọi là "Great Worm" (Sâu khổng lồ) do hậu quả nặng nề mà nó đã gây ra trên Internet khi đó, cả về tổng thời gian hệ thống không sử dụng được, lẫn về ảnh hưởng tâm lý đối với nhận thức về an ninh và độ tin cậy của Internet.

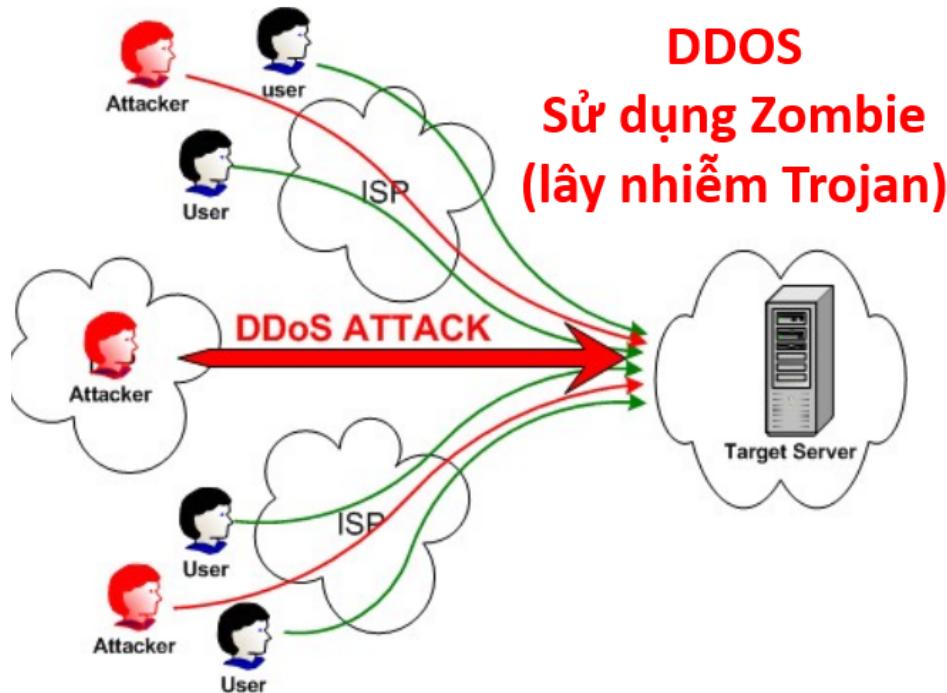
Sau này, kế thừa "thành tích này" một số sâu virus nổi tiếng khác cũng được sinh ra với các nhiệm vụ khác nhau

- Stuxnet : Tấn công cơ sở hạ tầng hạt nhân của Iran
- Melissa, Storm Worm
- Conflicker: Sâu máy tính lây nhiễm với tốc độ kinh khủng nhất toàn cầu, xuất hiện năm 2008

#### 4.2.4 Tấn công từ chối dịch vụ phân tán

Một cuộc tấn công từ chối dịch vụ (tấn công DoS - Viết tắt của Denial of Service) hay tấn công từ chối dịch vụ phân tán (tấn công DDoS - Viết tắt của Distributed Denial of Service) là một nỗ lực làm cho những người dùng không thể sử dụng tài nguyên của một máy tính. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống. Thủ phạm tấn công từ chối dịch vụ thường nhắm vào các trang mạng hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS root servers.

Một phương thức tấn công phổ biến kéo theo sự bão hòa máy mục tiêu với các yêu cầu liên lạc bên ngoài, đến mức nó không thể đáp ứng giao thông hợp pháp, hoặc đáp ứng quá chậm. Trong điều kiện chung, các cuộc tấn công DoS được bổ sung bởi ép máy mục tiêu khởi động lại hoặc tiêu thụ hết tài nguyên của nó đến mức nó không cung cấp dịch vụ, hoặc làm tắc nghẽn liên lạc giữa người sử dụng và nạn nhân.



Tấn công từ chối dịch vụ là sự vi phạm chính sách sử dụng internet của IAB (Internet Architecture Board) và những người tấn công hiển nhiên vi phạm luật dân sự.

US-CERT xác định dấu hiệu của một vụ tấn công từ chối dịch vụ gồm có:

- ✓ Mạng thực thi chậm khác thường khi mở tập tin hay truy cập Website;
- ✓ Không thể dùng một website cụ thể;
- ✓ Không thể truy cập bất kỳ website nào;
- ✓ Tăng lượng thư rác nhận được.

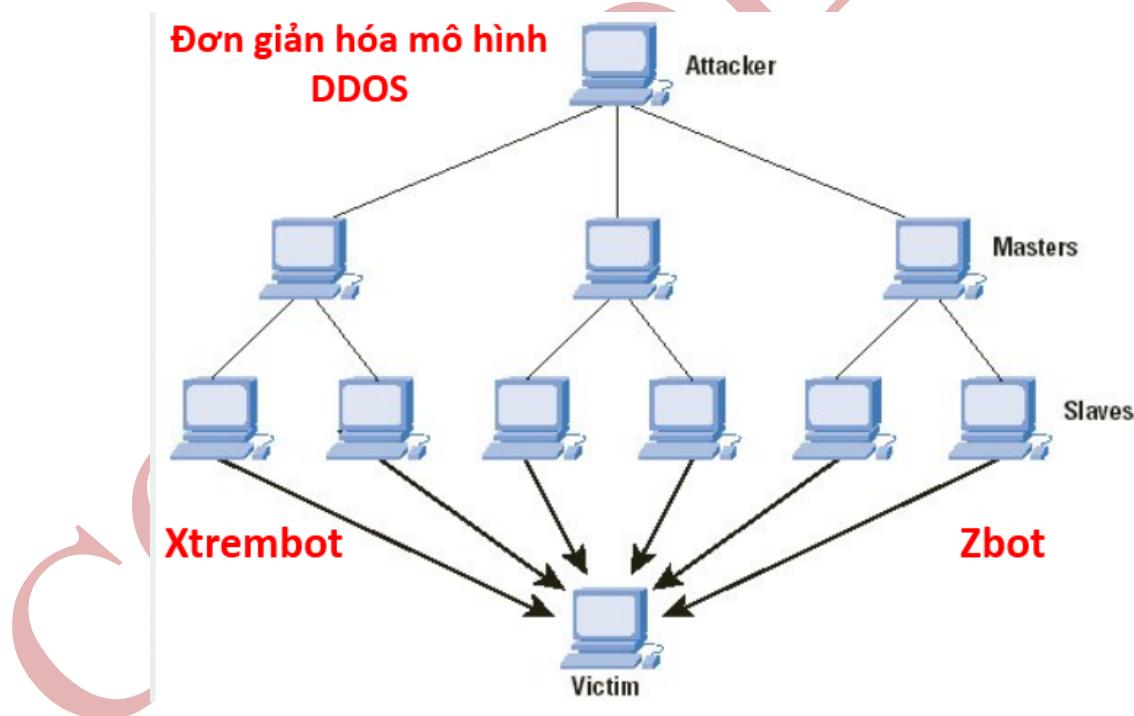
Không phải tất cả các dịch vụ đều ngừng chạy, thậm chí đó là kết quả của một hoạt động nguy hại, tật yếu của tấn công DoS. Tấn công từ chối dịch cũng có thể dẫn tới ván đè vè nhánh mạng của máy đang bị tấn công. Ví dụ băng thông của router giữa Internet và LAN

có thể bị tiêu thụ bởi tấn công, làm tổn hại không chỉ máy tính ý định tấn công mà còn là toàn thể mạng.

## Các phương thức tấn công

Tấn công từ chối dịch vụ là một loại hình tấn công nhằm ngăn chặn những người dùng hợp lệ được sử dụng một dịch vụ nào đó. Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm là tấn công vào các thiết bị định tuyến, web, thư điện tử và hệ thống DNS,...

- Tấn công vào giao thức: Tận dụng lỗ hổng của giao thức như cơ chế bắt tay ba bước, IP Spoofing...
- Tấn công vào băng thông: Làm cạn kiệt băng thông dựa trên lưu lượng gói tin chuyên vào lớn
- Tấn công vào ứng dụng: Lợi dụng lỗ hổng bảo mật để tấn công làm treo ứng dụng hoặc ép server khởi động lại.



Tấn công từ chối dịch vụ có thể được thực hiện theo một số cách nhất định. Có năm kiểu tấn công cơ bản sau đây:

- Nhầm tiêu tốn tài nguyên tính toán như băng thông, dung lượng đĩa cứng hoặc thời gian xử lý
- Phá vỡ các thông tin cấu hình như thông tin định tuyến
- Phá vỡ các trạng thái thông tin như việc tự động reset lại các phiên TCP.
- Phá vỡ các thành phần vật lý của mạng máy tính
- Làm tắc nghẽn thông tin liên lạc có chủ đích giữa các người dùng và nạn nhân dẫn đến việc liên lạc giữa hai bên không được thông suốt.

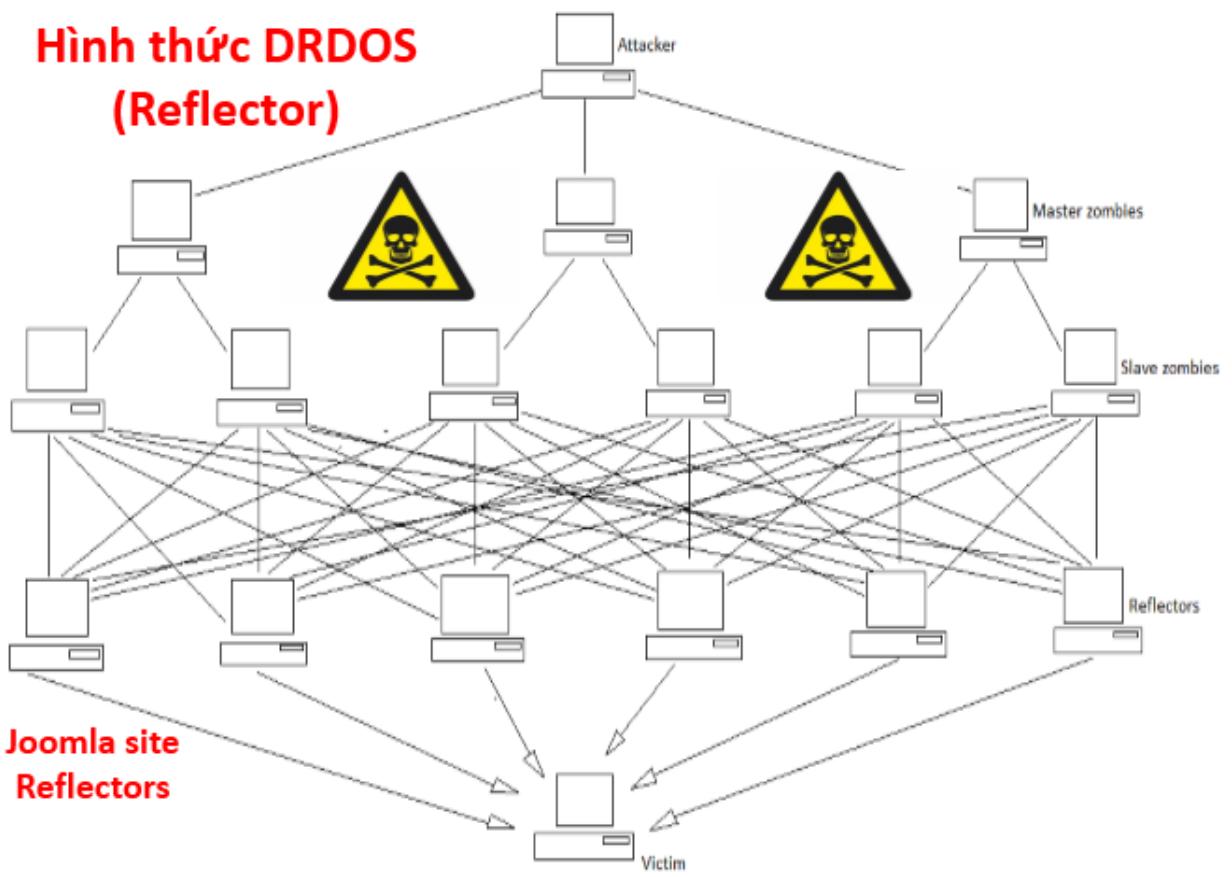
Một cuộc tấn công từ chối dịch vụ có thể bao gồm cả việc thực thi malware nhằm:

- Làm quá tải năng lực xử lý, dẫn đến hệ thống không thể thực thi bất kì một công việc nào khác.
- Những lỗi gọi tức thì trong microcode của máy tính.
- Những lỗi gọi tức thì trong chuỗi chỉ thị, dẫn đến máy tính rơi vào trạng thái hoạt động không ổn định hoặc bị đơ.
- Những lỗi có thể khai thác được ở hệ điều hành dẫn đến việc thiếu hụt tài nguyên hoặc bị thrashing. VD: như sử dụng tất cả các năng lực có sẵn dẫn đến không một công việc thực tế nào có thể hoàn thành được.
- Gây crash hệ thống.
- Tấn công từ chối dịch vụ iFrame: trong một trang HTML có thể gọi đến một trang web nào đó với rất nhiều yêu cầu và trong rất nhiều lần cho đến khi băng thông của trang web đó bị quá hạn.

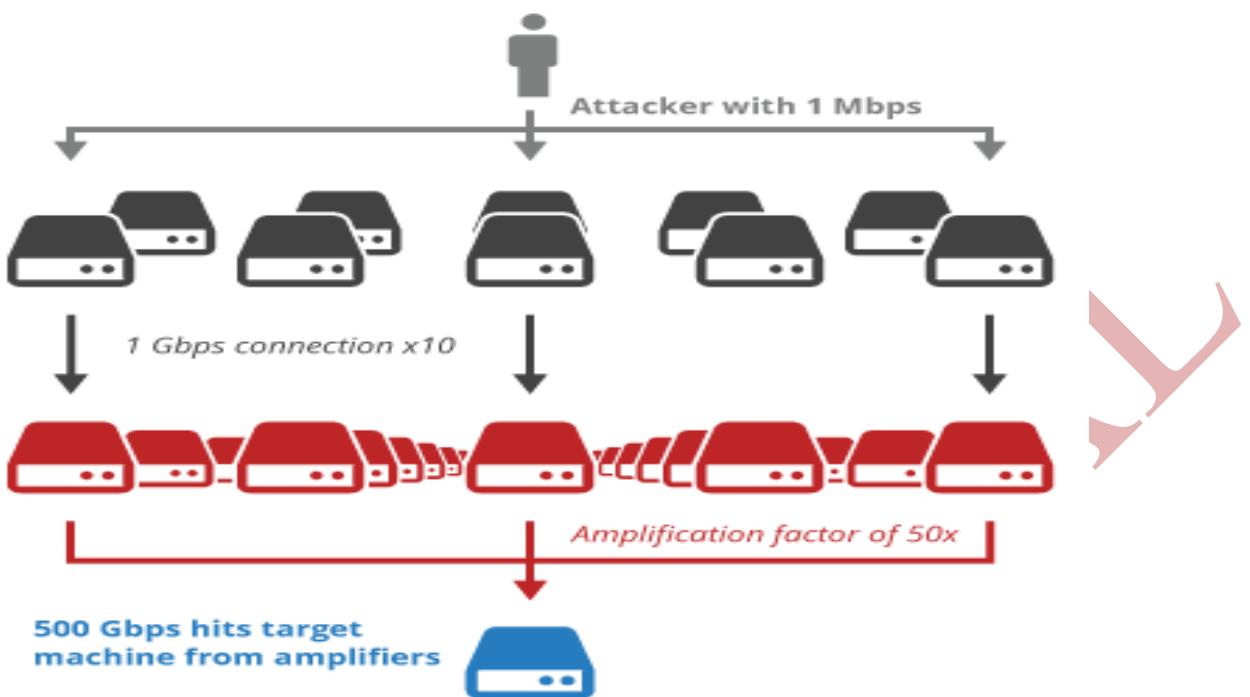
Một số dạng tấn công từ chối dịch vụ nguy hiểm

- DRDOS : Reflector DDoS là dạng tấn công sử dụng các Webserver mạnh bị lây nhiễm làm nguồn tấn công các máy chủ khác. Thông thường kẻ tấn công sẽ khai thác một lỗi trên CMS hoặc hệ quản trị phần mềm của những server này rồi chiếm quyền điều khiển

## Hình thức DRDOS (Reflector)



- NTP Attack hay tấn công khuếch đại dựa trên các máy chủ DNS và tỉ trọng giữa gói tin request và response của giao thức sử dụng. Sử dụng cơ chế này, kẻ tấn công có thể khuếch đại một kết nối lên gấp nhiều lần mà không cần phải có mạng lưới Zoombie khổng lồ.



Hiện nay kẻ tấn công cũng tiến hành khai thác các máy chủ Web có các CMS như Joomla, Wordpress tồn tại lỗ hổng bảo mật để làm trạm trung chuyển tấn công mới:



### 4.3 Tường lửa

Trong ngành mạng máy tính, bức tường lửa (tiếng Anh: firewall) là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

Tường lửa là một thiết bị phần cứng và/hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức, việc này tương tự với hoạt động của các bức tường ngăn lửa trong các tòa nhà. Tường lửa còn được gọi là Thiết bị bảo vệ biên giới (Border Protection Device - BPD), đặc biệt trong các ngữ cảnh của NATO, hay bộ lọc gói tin (packet filter) trong hệ điều hành BSD - một phiên bản Unix của Đại học California, Berkeley.

Nhiệm vụ cơ bản của tường lửa là kiểm soát giao thông dữ liệu giữa hai vùng có độ tin cậy khác nhau. Các vùng tin cậy (zone of trust) điển hình bao gồm: mạng Internet (vùng không đáng tin cậy) và mạng nội bộ (một vùng có độ tin cậy cao). Mục đích cuối cùng là cung cấp kết nối có kiểm soát giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên nguyên tắc quyền tối thiểu (principle of least privilege).

Cấu hình đúng đắn cho các tường lửa đòi hỏi kỹ năng của người quản trị hệ thống. Việc này yêu cầu hiểu biết đáng kể về các giao thức mạng và về an ninh máy tính. Những lỗi nhỏ có thể biến tường lửa thành một công cụ an ninh vô dụng.

Có 2 loại tường lửa thông dụng là tường lửa bảo vệ để bảo vệ an ninh cho máy tính cá nhân hay mạng cục bộ, tránh sự xâm nhập, tấn công từ bên ngoài và tường lửa ngăn chặn thường do các nhà cung cấp dịch vụ Internet thiết lập và có nhiệm vụ ngăn chặn không cho máy tính truy cập một số trang web hay máy chủ nhất định, thường dùng với mục đích kiểm duyệt Internet.

## Lịch sử

Ý tưởng đầu tiên được đã hình thành sau khi hàng loạt các vụ xâm phạm nghiêm trọng đối với an ninh liên mạng xảy ra vào cuối những năm 1980. Năm 1988, một nhân viên tại trung tâm nghiên cứu NASA Ames tại California gửi một bản ghi nhớ qua thư điện tử tới đồng nghiệp rằng: "Chúng ta đang bị một con VIRUS Internet tấn công! Nó đã đánh Berkeley, UC San Diego, Lawrence Livermore, Stanford, và NASA Ames." Con virus được biết đến với tên Sâu Morris này đã được phát tán qua thư điện tử và khi đó đã là một sự khó chịu chung ngay cả đối với những người dùng vô thường vô phạt nhất. Sâu Morris là cuộc tấn công diện rộng đầu tiên đối với an ninh Internet. Cộng đồng mạng đã không hề chuẩn bị cho một cuộc tấn công như vậy và đã hoàn toàn bị bất ngờ. Sau đó, cộng đồng Internet đã quyết định rằng ưu tiên tối cao là phải ngăn chặn không cho một cuộc tấn công bất kỳ nào nữa có thể xảy ra, họ bắt đầu cộng tác đưa ra các ý tưởng mới, những hệ thống và phần mềm mới để làm cho mạng Internet có thể trở lại an toàn.

Năm 1988, bài báo đầu tiên về công nghệ tường lửa được công bố, khi Jeff Mogul thuộc Digital Equipment Corp. phát triển các hệ thống lọc đầu tiên được biết đến với tên các tường lửa lọc gói tin. Hệ thống khá cơ bản này đã là thế hệ đầu tiên của cái mà sau này sẽ trở thành một tính năng kỹ thuật an toàn mạng được phát triển cao. Từ năm 1980 đến năm 1990, hai nhà nghiên cứu tại phòng thí nghiệm AT&T Bell, Dave Presotto và Howard Trickey, đã phát triển thế hệ tường lửa thứ hai, được biến đổi với tên các tường lửa tầng mạch (circuit level firewall). Các bài báo của Gene Spafford ở Đại học Purdue, Bill Cheswick ở phòng thí nghiệm AT&T và Marcus Ranum đã mô tả thế hệ tường lửa thứ ba, với tên gọi tường lửa tầng ứng dụng (application layer firewall), hay tường lửa dựa proxy (proxy-based firewall). Nghiên cứu công nghệ của Marcus Ranum đã khởi đầu cho việc tạo ra sản phẩm thương mại đầu tiên. Sản phẩm này đã được Digital Equipment Corporation's (DEC) phát hành với tên SEAL. Đợt bán hàng lớn đầu tiên của DEC là vào ngày 13 tháng 9 năm 1991 cho một công ty hóa chất tại bờ biển phía Đông của Mỹ.

Tại AT&T, Bill Cheswick và Steve Bellovin tiếp tục nghiên cứu của họ về lọc gói tin và đã phát triển một mô hình chạy được cho công ty của chính họ, dựa trên kiến trúc của thế hệ tường lửa thứ nhất của mình. Năm 1992, Bob Braden và Annette DeSchon tại Đại học

Nam California đã phát triển hệ thống tường lửa lọc gói tin thế hệ thứ tư. Sản phẩm có tên "Visas" này là hệ thống đầu tiên có một giao diện với màu sắc và các biểu tượng, có thể dễ dàng cài đặt thành phần mềm cho các hệ điều hành chẳng hạn Microsoft Windows và Mac/OS của Apple và truy nhập từ các hệ điều hành đó. Năm 1994, một công ty Israel có tên Check Point Software Technologies đã xây dựng sản phẩm này thành một phần mềm sẵn sàng cho sử dụng, đó là FireWall-1. Một thế hệ thứ hai của các tường lửa proxy đã được dựa trên công nghệ Kernel Proxy. Thiết kế này liên tục được cải tiến nhưng các tính năng và mã chương trình cơ bản hiện đang được sử dụng rộng rãi trong cả các hệ thống máy tính gia đình và thương mại. Cisco, một trong những công ty an ninh mạng lớn nhất trên thế giới đã phát hành sản phẩm này năm 1997.

Thế hệ FireWall-1 mới tạo thêm hiệu lực cho động cơ kiểm tra sâu gói tin bằng cách chia sẻ chức năng này với một hệ thống ngăn chặn xâm nhập.

### Các loại tường lửa

Có ba loại tường lửa cơ bản tùy theo:

- Truyền thông được thực hiện giữa một nút đơn và mạng, hay giữa một số mạng.
- Truyền thông được chặn tại tầng mạng, hay tại tầng ứng dụng.
- Tường lửa có theo dõi trạng thái của truyền thông hay không.

*Phân loại theo phạm vi của các truyền thông được lọc, có các loại sau:*

- Tường lửa cá nhân hay tường lửa máy tính, một ứng dụng phần mềm với chức năng thông thường là lọc dữ liệu ra vào một máy tính đơn.
- Tường lửa mạng, thường chạy trên một thiết bị mạng hay máy tính chuyên dụng đặt tại ranh giới của hai hay nhiều mạng hoặc các khu phi quân sự (mạng con trung gian nằm giữa mạng nội bộ và mạng bên ngoài). Một tường lửa thuộc loại này lọc tất cả truyền thông dữ liệu vào hoặc ra các mạng được kết nối qua nó. Loại tường lửa mạng tương ứng với ý nghĩa truyền thống của thuật ngữ "tường lửa" trong ngành mạng máy tính.

Khi phân loại theo các tầng giao thức nơi giao thông dữ liệu có thể bị chặn, có ba loại tường lửa chính:

- Tường lửa tầng mạng. Ví dụ iptables.
- Tường lửa tầng ứng dụng. Ví dụ TCP Wrappers.
- Tường lửa ứng dụng. Ví dụ: hạn chế các dịch vụ ftp bằng việc định cấu hình tại tệp /etc/ftpaccess.

Các loại tường lửa tầng mạng và tường lửa tầng ứng dụng thường trùng lênh nhau, mặc dù tường lửa cá nhân không phục vụ mạng, nhưng một số hệ thống đơn đã cài đặt chung cả hai.

Cuối cùng, nếu phân loại theo tiêu chí rằng tường lửa theo dõi trạng thái của các kết nối mạng hay chỉ quan tâm đến từng gói tin một cách riêng rẽ, có hai loại tường lửa:

- Tường lửa có trạng thái (Stateful firewall)
- Tường lửa phi trạng thái (Stateless firewall)

### Lý do sử dụng tường lửa

Mạng internet ngày càng phát triển và phổ biến rộng khắp mọi nơi, lợi ích của nó rất lớn. Tuy nhiên cũng có rất nhiều ngoại tác không mong muốn đối với các cá nhân là cha mẹ hay tổ chức, doanh nghiệp, cơ quan nhà nước... như các trang web không phù hợp lứa tuổi, nhiệm vụ, lợi ích, đạo đức, pháp luật hoặc trao đổi thông tin bất lợi cho cá nhân, doanh nghiệp... Do vậy họ (các cá nhân, tổ chức, cơ quan và nhà nước) sử dụng tường lửa để ngăn chặn.

Tường lửa đóng vai trò rất quan trọng để ngăn chặn các thành phần nguy hiểm như hacker, sâu, hay các loại virus trước khi chúng có thể xâm nhập vào máy tính của ta.

## **Chương 5: QUY TRÌNH THIẾT LẬP HỆ THỐNG AN NINH AN TOÀN**

### **5.1 Phân tích, xác định các mối đe dọa**

Một số mối đe dọa hàng đầu với an ninh hệ thống ngày nay bao gồm

#### **a) Mối đe dọa từ sự tấn công của Virus**

Hiện nay, Virus là mối hiểm họa hàng đầu đe dọa đến sự an toàn thông tin cho các tổ chức và các cá nhân tham gia hệ thống. Virus thế hệ mới có khả năng lây nhiễm và tốc độ phát tán cực kỳ nhanh, tần suất xuất hiện Virus mới ngày càng tăng cao. Virus thế hệ mới có nhiều dạng thức tấn công vào hệ thống như: chiếm dụng quyền kiểm soát máy tính làm bàn đạp tấn công từ chối dịch vụ (Denial of Service - DoS) vào những mục tiêu xác định, tạo ra các cửa hậu (Backdoor) trên máy tính để tạo điều kiện thuận lợi cho Hacker tấn công vào hệ thống, làm giảm hiệu suất của máy, làm giảm băng thông của hệ thống gây ách tắc trong quá trình trao đổi thông tin, làm sai lệch dữ liệu hoặc có thể nguy hiểm hơn là hành động xoá mất dữ liệu và làm hệ thống ngừng hoạt động.

#### **b) Hacker tấn công vào hệ thống**

Hacker có thể là một người bên ngoài hoặc cũng có thể là người bên trong tấn công vào hệ thống nhằm mục đích đạt được các ý đồ xấu như: ăn cắp thông tin, làm sai lệch thông tin theo chủ ý riêng hoặc phá hoại làm mất thông tin, ...

Ngày nay, có rất nhiều công cụ cho Hacker được cung cấp trên Internet và rất dễ sử dụng, do vậy một người bình thường cũng có thể trở thành một Hacker nguy hiểm đối với hệ thống. Một số công cụ thông thường như các chương trình lấy cắp Password trên mạng, các chương trình tạo Backdoor để thâm nhập và điều khiển máy mục tiêu, ...

Ngoài ra còn một số nguyên nhân khác gây mất an toàn cho hệ thống do lỗi của người sử dụng, do sự cố hỏng hóc thiết bị hoặc do các tai họa xảy ra như cháy nổ, động đất.

Mức độ quan tâm và đầu tư cho an ninh mạng tại các cơ quan, tổ chức

Thống kê trên cho thấy mức độ quan tâm đến các hệ thống bảo vệ an ninh mạng tại các cơ quan nhà nước và các doanh nghiệp tại Việt Nam là chưa cao. Đây chính là điều kiện thuận lợi cho các đối tượng tội phạm mạng thực hiện các hành vi tấn công, xâm hại.

Trong thời gian gần đây các loại tội phạm công nghệ cao tại Việt Nam phát triển cả về số lượng các cuộc tấn công cũng như chất lượng và gây ra những hậu quả nghiêm trọng hơn, phạm vi và quy mô lớn hơn. Hacker mũ đen/xám, các đối tượng này tấn công vào bất kỳ chỗ nào có thể, để phá hoại, để đánh cắp các thông tin, dữ liệu quý giá với đa phần là mục đích xấu. Không chỉ các cơ quan chính phủ của các nước mà nền CNTT đã phát triển mạnh bị hacker tấn công mà trong thời gian qua nhiều cơ quan nhà nước của Việt Nam cũng bị tấn công gây hậu quả về tài chính, kinh tế, làm tê liệt một phần không nhỏ tới công tác quản lý nhà nước và cao hơn nữa là làm ảnh hưởng tới uy tín của chính phủ Việt Nam trước cộng đồng quốc tế.

Nhiều cơ quan nhà nước tại Việt Nam vẫn chưa sử dụng mô hình quản lý bằng Domain cho hệ thống CNTT mà vẫn sử dụng Mạng ngang hàng (Workgroup). Điều đó có nghĩa các cán bộ quản trị mạng không phát huy được khả năng bảo vệ hệ thống và hỗ trợ người dùng khi các máy tính bị tấn công hoặc lây nhiễm virus trên diện rộng.

Do hạn chế của mô hình nói trên, người dùng máy tính trên hệ thống chỉ có thể quan tâm đến hiệu quả công việc nhưng chưa có đủ điều kiện để tuân thủ đầy đủ các quy định liên quan đến bảo mật an toàn thông tin. Đó là chưa kể đến việc, khi các máy tính chia sẻ tài nguyên ngang hàng, các thông tin sẽ có thể bị tiết lộ vì khi đã truy cập vào hệ thống thì có thể truy cập / chép dữ liệu từ các máy tính khác mà không có ai kiểm soát

## 5.2 Áp dụng cơ chế phòng thủ đa lớp

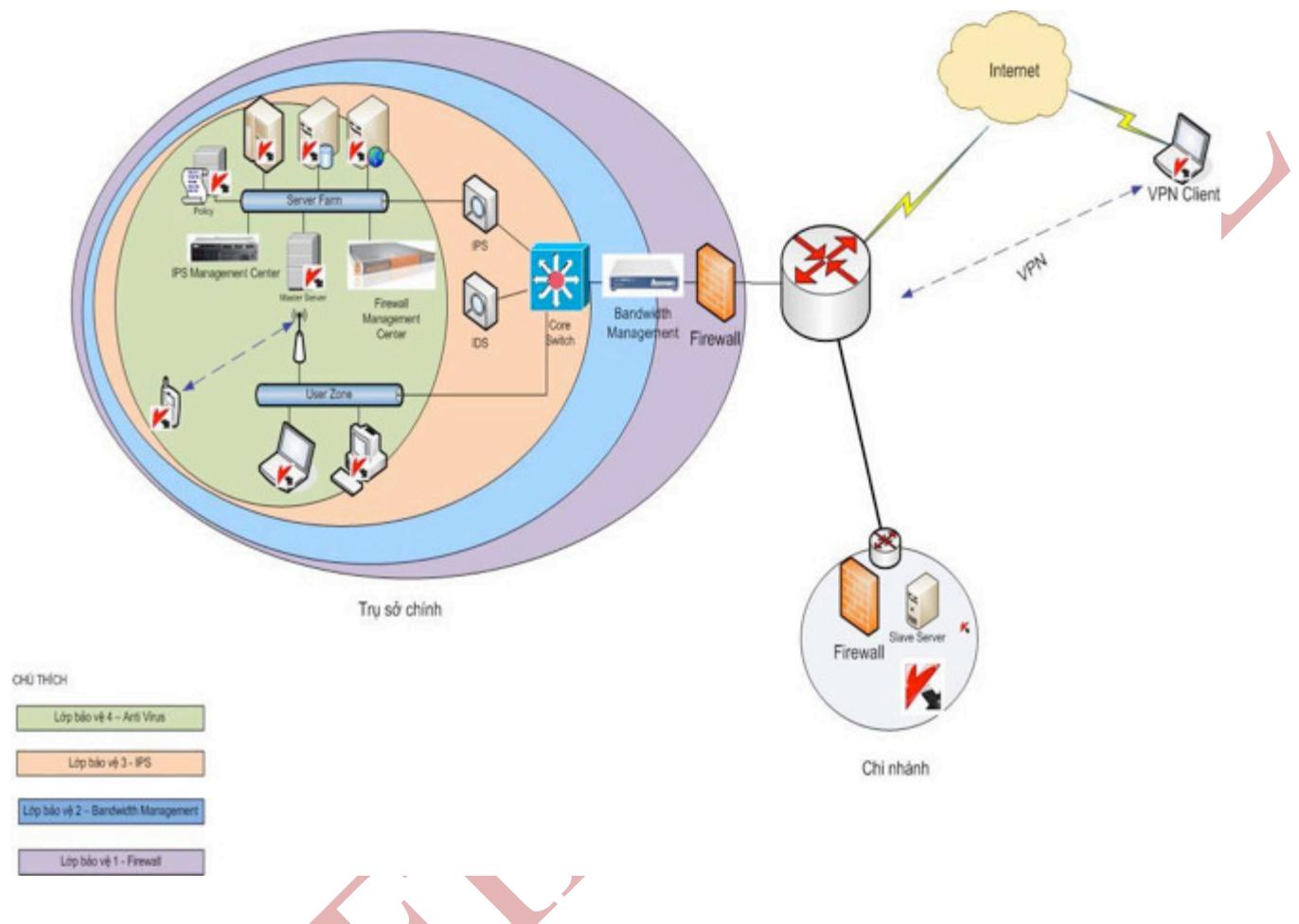
Phương án an ninh an toàn mạng cho doanh nghiệp/cơ quan/tổ chức – gọi tắt là tổ chức/doanh nghiệp - được xây dựng bao gồm nhiều lớp, bao gồm:

- ✓ Lớp 1: Gồm các Firewall (tường lửa) được đặt tại các cửa ngõ mạng, phân cách giữa mạng nội bộ của tổ chức với hệ thống mạng bên ngoài. Các Firewall có nhiệm vụ bảo vệ an ninh mạng vành đai ngoài. Các luồng dữ liệu trao đổi từ mạng bên ngoài đến mạng

nội bộ của tổ chức được lọc qua Firewall, chỉ các dữ liệu hợp lệ, đến từ các nguồn địa chỉ tin cậy mới được đi qua Firewall để vào trong mạng.

- ✓ Lớp 2: Gồm các thiết bị quản lý băng thông: Được đặt tại cửa ngõ kết nối ra internet và kết nối, thực hiện kiểm soát các giao thức, ứng dụng, dịch vụ trao đổi qua lại tại cửa ngõ mạng, ngăn chặn tình trạng tắc nghẽn mạng, đảm bảo chất lượng và sự ổn định cho các dịch vụ, ứng dụng trên mạng, đồng thời ưu tiên kết nối cho nhóm người dùng quan trọng của tổ chức.
- ✓ Lớp 3: Gồm các IPS (Intrusion Prevention System - thiết bị phòng chống xâm nhập) được đặt trước các vùng tài nguyên quan trọng của mạng (vùng máy chủ nội bộ) và IDS (Intrusion Detection System – thiết bị phát hiện và cảnh báo xâm nhập) trên các điểm nối giao thông trên mạng. IPS có nhiệm vụ:
  - Lắng nghe các gói tin trao đổi trên mạng, phân tích nội dung các gói tin để tìm ra các hành động xâm nhập, tấn công từ bên trong và bên ngoài mạng vào các vùng tài nguyên quan trọng, cảnh báo tới nhà quản trị mạng các dấu hiệu lạ thường trên mạng nhằm đưa ra biện pháp xử lý.
  - Rà soát và kiểm tra các điểm yếu trên các máy tính tham gia kết nối vào mạng, nơi dễ phát sinh các lỗ hổng an ninh mạng để các đối tượng xấu từ bên ngoài có thể khai thác, thực hiện các hành vi xâm nhập, trộm dữ liệu, phá hoại.
  - Tự động chống lại các hành vi xâm nhập tấn công trái phép vào các vùng tài nguyên quan trọng.
- ✓ Lớp 4: Hệ thống chương trình phòng chống virus, spam được cài đặt trên các máy chủ và máy trạm trên mạng. Chương trình phòng chống virus có nhiệm vụ quét và loại bỏ các đoạn mã độc hại (virus, spyware, trojan, adware, rootkit...), các email spam ra khỏi máy chủ và máy tính của người dùng, đảm bảo các dữ liệu lưu trữ trên máy chủ và máy tính trạm là được an toàn và bảo mật. Ngoài ra, người ta khuyến khích trang bị công cụ phục vụ lưu trữ, tổng hợp và phân tích thông tin của toàn hệ thống (SIEM), phục vụ tìm kiếm nguyên nhân ảnh hưởng đến an ninh, an toàn thông tin dựa trên các mối quan hệ tương quan giữa các sự kiện, hành động đã và đang xảy ra trên hệ thống. Công cụ giả lập tấn công cũng có thể được trang bị nhằm kiểm tra mức độ đảm bảo an toàn cho thông tin đối với các thiết bị hiện có trên hệ thống

Mô hình 4 lớp bảo vệ an ninh, an toàn mạng tại một tổ chức với hệ thống mạng gồm trung tâm và các chi nhánh, kết nối với nhau qua mạng WAN:



### 5.3 Mô hình phòng thủ thế hệ mới

Hiện nay, tội phạm mạng ngày càng trở nên tinh vi hơn, các kiểu tấn công như Trojans, DOS, Botnets. chỉ được sử dụng với các doanh nghiệp, tổ chức có quy mô nhỏ, không được đầu tư nhiều vào vấn đề bảo mật. Còn với những tập đoàn, tổ chức lớn, cơ quan chính phủ cần phải sử dụng các phương pháp tấn công tiên tiến mới mong xâm nhập vào được. Không có gì đảm bảo những công nghệ như Firewall, Antivirus, IPS. sẽ giữ cho hệ thống của bạn được an toàn. Những nhược điểm của chúng vẫn được biết đến như:

- Antivirus (diệt virus): chưa từng được coi là giải pháp tuyệt đối an toàn cho toàn bộ hệ thống, Phần mềm được cài đặt trên các máy cá nhân nhằm hỗ trợ tâm lý an toàn

cho người dùng và tin tức có vô vàn cách "qua mặt" các phần mềm Antivirus hiện nay.

- Firewall: không đủ thông minh để hiểu từng loại thông tin và phân tích chúng mà chỉ có thể ngăn chặn sự xâm nhập khi đã xác định rõ các thông số; không thể chống lại các cuộc tấn công bằng dữ liệu hay rò rỉ thông tin hoặc xâm nhập từ nội bộ.
- IPS: giải pháp này khắc phục được nhiều hạn chế nhưng chúng vẫn có thể gây ra tình trạng phát hiện nhầm, có thể không cho phép truy cập hợp lệ tới hệ thống.

Đối với tội phạm mạng tinh vi, chúng ta cần có phương án mạnh mẽ hơn và khái niệm phương pháp phòng chống các mối đe dọa an ninh tiên tiến (ATD) ra đời.

ATD (Advanced Threat Defense) là phương pháp phòng chống các mối đe dọa an ninh mạng tiên tiến để chống lại cách thức tấn công có chủ đích APT (Advanced Persistent Threat), những lỗ hổng zero-day. Thực ra, mối quan tâm chính của ATD là APT, bởi đây là công nghệ tấn công tiên tiến mà những phương pháp bảo mật truyền thống chưa giải quyết được.

Để hiểu rõ ATD, ta cũng cần biết về "kẻ thù" chính mà nó phải đối mặt - APT. APT là hình thức tấn công dai dẳng, tập trung, có chủ đích, được thiết kế riêng cho từng mục tiêu, để xâm nhập vào đối tượng có chứa dữ liệu nhầm tìm kiếm các thông tin giá trị và gửi ra cho đối tượng bên ngoài. Việc thâm nhập vào các hệ thống phòng thủ của một tổ chức hay quốc gia cụ thể để đánh cắp thông tin mà không bị phát hiện đòi hỏi thời gian nghiên cứu và thực hiện trong vài tháng, thậm chí là vài năm, dưới sự phối hợp của một tổ chức gồm những chuyên gia hàng đầu. Chính vì chi phí cũng như phạm vi và thời gian tham gia, APT thường được khởi xướng nhằm vào những tổ chức lớn, cơ quan chính phủ. Các vụ thất thoát dữ liệu như vậy đã từng xảy ra với RSA, CitiBank và Global Payments.

Thế giới cũng đã được chứng kiến những vụ tấn công APT gây hậu quả nghiêm trọng. Năm 2010, sâu Stuxnet tấn công hơn 1.000 máy ly tâm trong chương trình hạt nhân của Iran, làm chúng ngừng hoạt động hoàn toàn. Hay sâu Hydraq được sử dụng để khai thác lỗ hổng trên trình duyệt Internet Explorer, nhằm đánh cắp dữ liệu như tài khoản ngân hàng,

mật khẩu đăng nhập, hợp đồng kinh doanh, danh sách khách hàng, dữ liệu, văn bản quan trọng của nạn nhân trong nhiều tháng trời.

Ngoài APT, các dòng sản phẩm của nhiều hãng bảo mật còn hỗ trợ chống lại lỗ hổng zero-day. Zero-day là một thuật ngữ chỉ những lỗ hổng chưa được công bố hoặc chưa khắc phục. Lợi dụng những lỗ hổng này, hacker có thể xâm nhập vào hệ thống của các doanh nghiệp, tổ chức nhằm đánh cắp hay thay đổi dữ liệu. Tuổi thọ trung bình của một lỗ hổng zero-day là 348 ngày, thậm chí có những lỗ hổng tồn tại hơn 1.000 ngày, tương đương gần 3 năm mà chưa bị phát hiện.

Chính vì những mối nguy hiểm như trên, yêu cầu về một sản phẩm chống lại chúng đặt ra bài toán không hề dễ đối với các hãng bảo mật, khi mà Firewall, IPS vẫn còn bộc lộ nhiều khuyết điểm.

### **Nhiệm vụ chính của hệ thống ATD**

Khi đã triển khai các giải pháp ATD trên toàn bộ hệ thống, chúng phải đảm bảo hai nhiệm vụ chính như sau:

- Phát hiện và ngăn chặn các mối đe dọa để bảo vệ hệ thống khỏi các cuộc tấn công trong nội bộ cũng như từ bên ngoài. Yêu cầu kỹ thuật then chốt ở đây là hệ thống ATD phải có khả năng xác định các mối đe dọa trong thời gian thực - khi chúng xảy ra - và chủ động có hành động phòng ngừa khi phát hiện ra chúng. Khả năng này rất quan trọng bởi vì trong nhiều trường hợp, hệ thống ATD là chốt chặn duy nhất trong cơ sở hạ tầng an ninh mạng, có thể xác định chính xác các mối đe dọa cũng như ngăn chặn nó mà không làm gián đoạn việc lưu thông trong mạng.

- Ứng phó trong mọi tình huống giúp tự động khắc phục và đẩy nhanh chu trình ứng cứu khi có sự cố. Trong vai trò này, hệ thống ATD phải có khả năng phát hiện ra hệ thống bị xâm nhập, điều tra các mối đe dọa đang hoạt động cũng như "ngủ đông", bao gồm cả mục tiêu mà chúng sẽ hướng tới trước khi dữ liệu bị mất. Có một thực tế là không có sản phẩm ATD nào đảm bảo chắc chắn hệ thống an toàn trước những kỹ thuật tiên tiến mới phát triển, nhất là chúng lại được tạo ra cho các mục tiêu đã xác định trước. Do đó, chúng phải đảm bảo có bộ nhớ cho việc lưu trữ thông tin mã độc phục vụ cho

công tác tìm kiếm, truy vấn và phân tích, cũng như cập nhật thường xuyên thông tin về các mã độc trên toàn thế giới, đồng thời cung cấp khả năng ứng cứu khẩn cấp, nhanh chóng khi có xâm nhập.

## Những yêu cầu đối với giải pháp ATD

Một giải pháp ATD toàn diện cần đảm bảo ba yêu cầu sau:

- ✓ Chống lại những mối đe dọa: Giải pháp ATD thực sự cần cung cấp khả năng chống lại các cuộc tấn công nhằm vào từng giai đoạn của vòng đời APT: trước khi tải về, khi chúng lưu thông trong mạng cho đến khi chúng đã được cài đặt trên thiết bị đầu cuối. Để làm được điều đó, giải pháp ATD cần có các tính năng:
  - Nâng cao khả năng phát hiện phần mềm độc hại: Phân tích liên tục dòng dữ liệu đi qua mạng, duy trì khả năng phát hiện với tỉ lệ sai sót thấp.
  - Giám định phần mềm độc hại: Mô tả chi tiết các phần mềm độc hại nhờ môi trường ảo hóa được tạo ra trước đó để nắm rõ cách đăng nhập, thay đổi tập tin, thay đổi cách vận hành hệ thống, cách đưa dữ liệu ra ngoài...
  - Phòng chống các nguy cơ tại thời gian thực: Phân tích lưu lượng mạng, cung cấp khả năng phát hiện và phòng ngừa ngay tức khắc.
  - Tự động nhận biết các mối đe dọa: Nhanh chóng xác định các hoạt động đáng ngờ và nguy hiểm, đồng thời tự động tiêu diệt những mối đe dọa đã từng được hệ thống biết tới.
  - Chính sách linh hoạt: Có khả năng áp dụng các chuẩn mã nguồn mở, ví dụ như YARA (YARA là một công cụ mã nguồn mở đa nền tảng được thiết kế để giúp các chuyên gia bảo mật xác định và phân loại phần mềm độc hại).
  - Hiệu suất cao: Đảm bảo phân tích lưu lượng cao (hàng Gigabit) trong thời gian thực mà vẫn cung cấp khả năng hiển thị, phân tích và bảo vệ khỏi các mối đe dọa trước khi chúng có thể gây tổn hại cho tổ chức.
    - Bảo vệ dữ liệu khỏi bị đánh cắp

- Một giải pháp toàn diện ATD thực sự sẽ trực tiếp phát hiện và ngăn chặn việc tiếp cận trái phép các thông tin nhạy cảm, có giá trị. Các yêu cầu kỹ thuật cần có bao gồm:
  - Kiểm soát luồng dữ liệu: Bằng cách sử dụng những luật và kỹ thuật phức tạp để ngăn chặn các hành vi trộm cắp dữ liệu nhạy cảm và bí mật ra khỏi mạng thông tin.
  - Hiển thị nội dung: Cung cấp khả năng hiển thị, phân tích và kiểm soát tất cả các giao thức, ứng dụng và các loại tập tin để bảo vệ chống lại các mối đe dọa tiên tiến và ngăn chặn hành vi trộm cắp dữ liệu trong thời gian thực.
  - Hỗ trợ phân loại dữ liệu: Thông qua những cơ chế linh hoạt, bạn có thể xác định các đặc tính của dữ liệu có giá trị tại mức nào sẽ được coi là nhạy cảm và tránh cho chúng đi ra khỏi hệ thống mạng.
  - Cảnh báo: Cung cấp khả năng cảnh báo toàn diện, thông tin về các hoạt động cho phép bạn phân loại nhanh chóng và khắc phục các mối đe dọa.

### Phân tích được các vấn đề an ninh mạng

Một giải pháp ATD toàn diện còn cung cấp hồ sơ lịch sử của tất cả các hoạt động mạng, do đó, bạn có thể "quay ngược thời gian" để tìm kiếm những mối đe dọa mà hệ thống không hề biết tại thời điểm đó. Các yêu cầu kỹ thuật gồm có:

- Ghi lại đầy đủ dữ liệu: Thu thập thông tin chi tiết (siêu dữ liệu) về tất cả các giao dịch trong mạng. Siêu dữ liệu này được lưu trữ trong bộ nhớ hệ thống và làm cơ sở cho việc phát hiện sau này.
- Phân tích đa chiều: Phân tích nội dung và so sánh với nhiều nguồn khác nhau như lịch sử của hệ thống, các chính sách được cài đặt sẵn cũng như các mối đe dọa được cập nhật thường xuyên từ các tổ chức khác.
- Tổng kết: Tự động cung cấp bản tổng kết và xu hướng trong hệ thống về các yếu tố như máy chủ, các cảnh báo, vị trí hay các giao thức để có cái nhìn tổng quan về những mối đe dọa đối với doanh nghiệp, tổ chức.

- Báo cáo linh hoạt: Có khả năng đưa ra những bản báo cáo theo tiêu chuẩn hay tùy chỉnh riêng dựa vào siêu dữ liệu được thu thập theo thời gian.
- Cảnh báo nguy cơ: Với những giao dịch có nhiều nét tương đồng với các mối đe dọa đã được biết đến cần cảnh báo cho nhân viên quản trị biết và có hướng xử lý.

## Một số giải pháp ATD từ các hãng bảo mật

Dựa trên những yêu cầu về một sản phẩm ATD, các hãng bảo mật đã nghiên cứu và cho ra đời các giải pháp của riêng mình. Có thể kể đến một vài cái tên nổi tiếng như: McAfee, Trend Micro, Cyphort, General Dynamics...

McAfee đã tích hợp phương pháp phòng chống tiên tiến vào sản phẩm McAfee Advanced Threat Defense (McAfee ATD) của mình với hai phiên bản mang tên ATD-3000 và ATD-6000. Đồng thời, McAfee ATD có thể kết hợp với các sản phẩm khác để cung cấp cho bạn một cơ chế bảo vệ đa lớp chống lại phần mềm độc hại. Các tính năng của McAfee ATD hỗ trợ gồm:

- Cơ chế phát hiện sơ bộ của nó chứa một danh sách đen (black list) các phần mềm độc hại đã được biết đến để nhanh chóng phát hiện ra chúng.
- Tích hợp McAfee GTI (McAfee Global Threat Intelligence) hỗ trợ việc tra cứu trên đám mây (cloud) nhằm sớm phát hiện phần mềm độc hại được xác định bởi các tổ chức trên toàn thế giới.
- Có công McAfee Anti-Malware để hỗ trợ khả năng mô phỏng.
- Tự động phân tích các tập tin bằng cách thực hiện nó trong một môi trường sandbox ảo (Sandbox là một kỹ thuật quan trọng trong lĩnh vực bảo mật có tác dụng cô lập các ứng dụng, ngăn chặn các phần mềm độc hại để chúng không thể làm hỏng hệ thống máy tính, hay cài cắm các mã độc nhằm ăn cắp thông tin cá nhân của bạn). Căn cứ vào cách các tập tin phản ứng lại, McAfee ATD sẽ xác định tính chất nguy hiểm của nó.

Trend Micro có giải pháp Deep Discovery, được tạo thành bởi 2 công cụ Deep Discovery Inspector (DDI - nhằm giám sát lưu lượng mạng, phát hiện và bảo vệ chống lại tấn công APT, phishing, lỗ hổng zero-day .) và Deep Discovery Advisor (DDA - có chức

năng phân tích chuyên sâu các mẫu đáng ngờ bằng cách sử dụng phương pháp phân tích Heuristic, cung cấp khả năng phân tích và báo cáo thông minh để chống lại các botnet và mã độc). Cùng với 2 công cụ này, giải pháp Websense Content Security với công nghệ lọc nội dung (ACE - Advanced Classification Engine) gồm nhiều phương pháp lọc và phân loại sẽ hỗ trợ kiểm tra, phát hiện và chống lại các mối đe dọa xâm nhập vào hệ thống.

Hãng Cyphort có giải pháp phân phối trên nền tảng Cyphort Advanced Threat Defense như phần mềm có thể cài đặt trên các thiết bị phần cứng thông thường, máy ảo và môi trường đám mây. Cyphort ATD bao gồm bốn thành phần cốt lõi:

- Cyphort Collectors: Thiết bị dò được triển khai ở tất cả các điểm quan trọng trên khắp cơ sở hạ tầng mạng doanh nghiệp để thu thập các thông tin đáng ngờ.
- Cyphort Core: Giữ nhiệm vụ phân tích những đối tượng tình nghi được Cyphort Collectors gửi đến.
- Cyphort Manager: Quản lý trên giao diện web, cho phép việc giám sát triển khai toàn bộ hệ thống và cung cấp quyền truy cập tới các tính năng cũng như báo cáo.
- Cyphort Threat Network: Dịch vụ đám mây để các Cyphort Core trao đổi thông tin với nhau nhằm cập nhật những mối đe dọa được phát hiện trên toàn cầu.
- Ngoài ra, nhiều hãng bảo mật khác cũng có những giải pháp của riêng mình, như General Dynamics với giải pháp Fidelis Cybersecurity hay Cipher với Cypher ATD...

Chi phí cho các thiết bị không hề nhỏ, dao động từ khoảng 20.000 USD đến hàng trăm ngàn USD tùy thuộc vào từng hãng. Với những phương pháp tấn công truyền thống đã có nhiều phương án giải quyết như Firewall, IPS, IDS, Anti-virus..., tuy nhiên sự nguy hiểm thật sự đối với các tổ chức, doanh nghiệp lớn, các cơ quan chính phủ hiện nay đến từ các phương pháp tấn công tiên tiến. Vì vậy, rất nên xem xét khả năng áp dụng các giải pháp ATD nếu tổ chức cảm thấy đủ điều kiện để triển khai trên hệ thống của mình.

#### **5.4 Đào tạo con người**

**Tại sao lại là con người?**

Trong tất cả các mối đe dọa về an toàn thông tin thì có thể chính bạn mới là nhân tố đe dọa lớn nhất trước nguy cơ bảo mật mạng. Dễ dàng nhất như việc kích lên các kết nối trong thư rác, download các file chia sẻ và phần mềm miễn phí hay việc cắm USB vào máy tính không kiểm tra kỹ là những hành động vô cùng nguy hiểm trên internet. Vô tình chỉ một sơ suất nhỏ trong hành vi của con người, lãnh đạo một tổ chức, nhân viên kỹ thuật cũng có thể làm lây nhiễm virus tới toàn bộ hệ thống hoặc phá vỡ quy trình đảm bảo an toàn cho toàn mạng.

Ngoài việc đầu tư một phần mềm tốt nhất và cập nhật nó một cách thường xuyên, chúng ta cần có những hướng dẫn và giáo dục chính quy tới đội ngũ nhân viên, nhân lực làm việc về tầm quan trọng của những thói quen, quy trình xử lý tác nghiệp được chuẩn hóa theo phương thức đảm bảo an toàn thông tin. Các thỏa thuận mua bán, giao dịch trực tuyến bạn cũng nên tránh hoặc ít nhất là chúng ta cần hiểu được các bước thực hiện an toàn trước khi tiến hành giao dịch. Ngoài ra, không bao giờ download bất cứ thứ gì được gửi tới trong mail trừ khi bạn có thể kiểm tra và quét virus, spyware trước cho nó. Tuy vậy, trong thời buổi số hiện nay, việc chia sẻ thông tin trên internet là việc thường xuyên, có thể là việc mua bán tranh ảnh, các bộ phim hay các file mà không có gì đảm bảo.

### **Đào tạo như thế nào?**

Hiện nay, tất cả các cường quốc mạnh về an toàn thông tin và chiến tranh thông tin đều có đội ngũ nhân lực đào tạo có kỹ năng tốt về lập trình, an ninh mạng và có những sách trắng hướng dẫn cụ thể tới từng công ty, tổ chức, cơ quan hành chính nhà nước phải tuân theo trong quy trình xử lý dữ liệu nội bộ. Quy trình đào tạo bài bản về con người có thể tuân theo một số phương cách sau

- Đào tạo chính quy
- Đào tạo ngắn hạn thông qua các chứng chỉ bảo mật uy tín CEH, MCSA
- Đào tạo ngắn hạn thông qua tập huấn và tài liệu hướng dẫn trực quan
- Tổ chức quy tắc và chính sách an toàn thông tin nội bộ trong cơ quan

Dù tuân theo bất cứ phương cách nào thì nhân tố con người và mức độ tiếp thu, nhận thức và thực hiện đóng vai trò vô cùng quan trọng để đảm bảo một hệ thống an toàn toàn diện.

Con người dù sao cũng là giải pháp linh hoạt nhất có thể phản ứng nhanh với hầu hết các mối đe dọa, đôi khi có thể cứu thua được những thiệt hại trông thấy nếu anh ta có hiểu biết sâu về an ninh và làm chủ được hệ thống.

CONFIDENTIAL