Chương trình KC-01:
Nghiên cứu khoa học
phát triển công nghệ thông tin
và truyền thông

Đề tài KC-01-01:
Nghiên cứu một số vấn đề bảo mật và
an toàn thông tin cho các mạng dùng
giao thức liên mạng máy tính IP

**Báo cáo kết quả nghiên cứu**

# GIỚI THIỆU MỘT SỐ KẾT QUẢ MỚI TRONG BẢO MẬT MẠNG DÙNG GIAO THỨC IP, AN TOÀN MẠNG VÀ THƯƠNG MẠI ĐIỆN TỬ

Quyển 1A: Giới thiệu công nghệ IPSEC,
công nghệ phát hiện xâm nhập và thương mại điện tử"

HÀ NỘI-2002

**Báo cáo kết quả nghiên cứu**

# GIỚI THIỆU MỘT SỐ KẾT QUẢ MỚI TRONG BẢO MẬT MẠNG DÙNG GIAO THỨC IP, AN TOÀN MẠNG VÀ THƯƠNG MẠI ĐIỆN TỬ

Quyển 1A: Giới thiệu công nghệ IPSEC,
công nghệ phát hiện xâm nhập và thương mại điện tử"

**Chủ trì nhóm nghiên cứu**
**PGS, TS Hoàng Văn Tảo**

# MỤC LỤC

**Chương 1.** GIỚI THIỆU VỀ IPSEC
1. IPSEC là gì
2. Các đặc tính
3. Cài đặt và các cấu trúc
4. Dùng IPSEC ở đâu
5. ưu điểm của IPSEC
6. Các hạn chế của IPSEC
7. Cách dùng IPSEC
8. Kết luận
Tài liệu tham khảo

**Chương 2.** PHÁT HIỆN XÂM NHẬP: LÀM THẾ NÀO ĐỂ TẬN DỤNG MỘT CÔNG NGHỆ VẪN CÒN NON NỚT
1. Về phát hiện xâm nhập
2. Các giải pháp phát hiện xâm nhập
3. Những ưu điểm và hạn chế của công nghệ phát hiện xâm nhập
4. ước định các yêu cầu phát hiện xâm nhập
5. Khai thác kiến trúc phát hiện xâm nhập
6. Kết luận
Tài liệu tham khảo

**Chương 3.** THƯƠNG MẠI ĐIỆN TỬ
1. Một số khái niệm cơ bản về thương mại điện tử ( TMĐT )
2. Tình hình phát triển TMĐT trên thế giới
3. Tình hình phát triển TMĐT ở Việt Nam
4. An toàn trong TMĐT
Tài liệu tham khảo

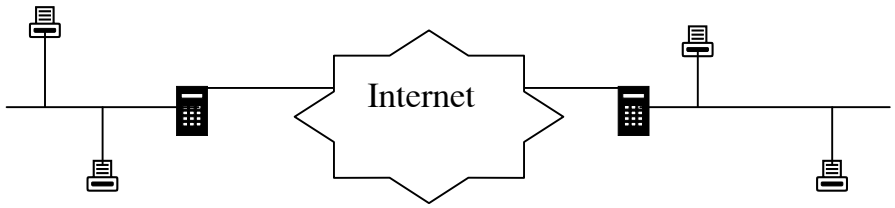
Phụ lục. IBM đạt được bước tiến mới trong chế tạo máy tính lượng tử

# CHƯƠNG 1
# GIỚI THIỆU VỀ IPSEC

## 1-IPSEC là gì?

IPSEC là từ viết tắt của Internet Protocol SECurity. Nó sử dụng mật mã để cung cấp đồng thời 2 dịch vụ xác thực và bảo mật. Việc xác thực đảm bảo rằng các gói tin được gửi đi từ người gửi đích thực và không bị thay đổi trên đường đi. Việc mã hóa chống lại ý định đọc trộm nội dung của các gói tin. IPSEC có thể bảo vệ bất kỳ một thủ tục nào dựa trên IP và bất kỳ một môi trường nào được sử dụng dưới tầng IP. IPSEC còn có thể cung cấp một số dịch vụ bảo mật ở mức "nền tảng", không ảnh hưởng gì đối với người sử dụng. Hơn thế nữa, nó có thể bảo vệ cả việc pha trộn các thủ tục chạy trên tổ hợp môi trường phức tạp (ví dụ như IMAP/POP) mà không cần thay đổi chúng bất cứ điểm gì, bởi vì việc mã hóa xảy ra ở tầng IP.

Các dịch vụ IPSEC cho phép bạn xây dựng các đường ngầm an toàn thông qua các mạng chưa được tin. Bất kỳ một cái gì đi qua mạng chưa được tin cậy sẽ được mã hóa bởi máy IPSEC gateway (máy cửa ngõ) và được giải mã bằng máy cửa ngõ ở đầu đằng kia của đường truyền. Kết quả là chúng ta thu được một mạng riêng ảo (Virtual Private Network-VPN). Đó là một mạng được bảo mật hoàn toàn mặc dù nó bao gồm nhiều máy tại nhiều điểm được nối với nhau bằng Internet.




VPN

## 2- Các đặc tính

Nhiệm vụ của IPSEC được chuyển hóa thành những đặc tính kiến trúc chủ chốt sau.

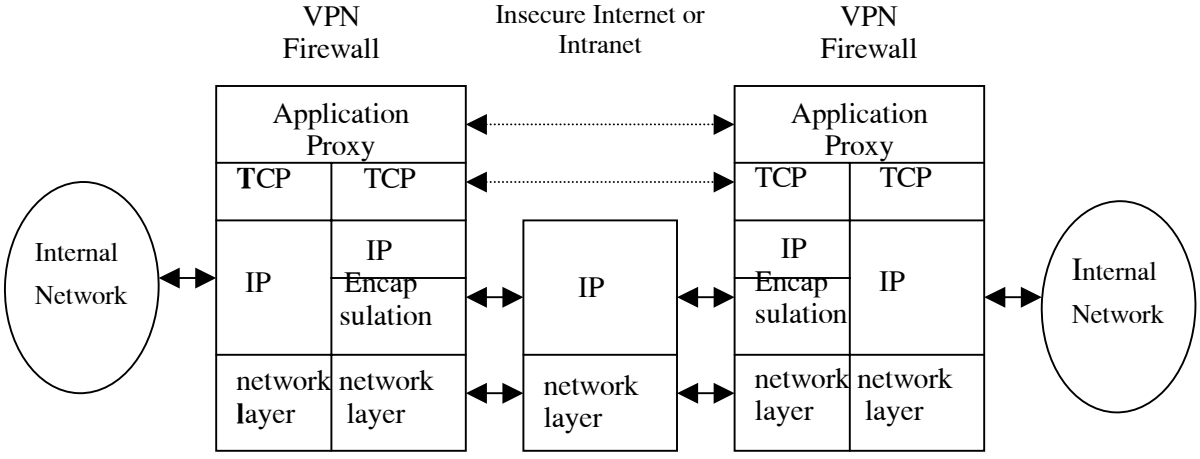
### *2.1- Phân tách các chức năng xác thực và bảo mật bằng sự độc lập biến đổi*

Các dịch vụ bảo mật và xác thực là độc lập với nhau. Điều này làm đơn giản hóa việc cài đặt và giảm ảnh hưởng thi hành của nó đối với hệ thống. Nó cũng đem lại cho người sử dụng khả năng lựa chọn mức bảo vệ thích hợp cho giao dịch của họ. Các chức năng bảo mật là độc lập với các biến đổi mật mã. Điều này

cho phép các công nghệ mật mã mới có thể tích hợp vào IPSEC mà không cần thay đổi kiến trúc cơ sở và tránh xung đột giữa việc sử dụng đặc biệt-tại chỗ với hạn chế xuất khẩu. Nó cũng làm cho người sử dụng cuối cùng có thể áp dụng biến đổi trùng hợp tốt nhất với các yêu cầu bảo mật của riêng mình. Người sử dụng có thể chọn các dịch vụ xác thực sử dụng hàm băm mật mã có giá cài đặt thấp, ảnh hưởng thi hành nhỏ và ít hạn chế sử dụng quốc tế. Những cài đặt này có thể được phân phối rộng rãi và cung cấp tiến bộ từng bước về bảo mật cho phần lớn các giao dịch Internet hiện nay. Hoặc là, người sử dụng có thể chọn các hàm mật mã dựa trên mật mã khóa bí mật. Như thế sẽ khó cài đặt hơn, có ảnh hưởng thi hành lớn hơn và thường là đối tượng của giới hạn sử dụng quốc tế, cho nên mặc dù nó cung cấp mức độ mật cao hơn, việc phân phối chúng luôn bị giới hạn. Hoặc là họ có thể tổ hợp những hàm này để đảm bảo mức bảo mật cao nhất có thể được.

### *2.2- Cài đặt ở tầng mạng (network layer) cùng với thiết lập một chiều*

Việc đưa chức năng bảo mật vào tầng mạng có nghĩa là mọi giao thức IP trên máy có thể hoạt động có bảo mật mà không cần sự can thiệp của từng người riêng biệt. Các giao thức dẫn đường như Giao thức Cổng Ngoài (Exterior Gateway Protocol -EGP) và Giao thức Cổng Biên (Border Gateway Protocol- BGP) cũng như các giao thức vận tải có kết nối (connection) và không cần khẳng định kết nối (connectionless) như TCP hay UDP đều có thể bảo mật. Các ứng dụng sử dụng các thủ tục máy trạm này không cần phải thay đổi gì vẫn có được các ưu việt của dịch vụ IPSEC. Các dịch vụ IPSEC thêm vào khả năng bảo mật các ứng dụng có khả năng tổn thương tiềm tàng (ví dụ, như mật khẩu rõ) bằng một lần sửa đổi hệ thống. Và lần sửa đổi này sẽ bảo mật tất cả các ứng dụng như vậy không phụ thuộc vào dịch vụ IP hay các vận chuyển mà nó sử dụng.




VPN và mô hình TCP/IP

Khả năng này có thể mở rộng đến dịch vụ dòng bằng các gói multicast hoặc unicast, khi đó địa chỉ đích là không xác định. IPSEC có thể làm được điều này bằng một lược đồ khởi tạo một hướng (unidirectorial) để thiết lập liên kết bảo mật. Trạm gửi chuyển chỉ số thiết lập đến trạm nhận. Trạm nhận sử dụng chỉ số này để truy cập vào bảng các tham số bí mật chi phối mối liên kết. Trạm nhận không cần phải tương tác với trạm gửi để thiết lập kết nối mật theo một hướng. Với các liên kết hai chiều, quá trình cần có chiều ngược lại. Trạm nhận trở thành trạm gửi, chuyển chỉ số thiết lập ngược về người khởi đầu. Các trạm nhận và gửi hoặc thể là máy chủ hoặc là cổng an ninh.

### *2.3- Liên kết của máy và cổng (host and gateway)*

IPSEC hỗ trợ hai dạng kết nối cơ bản, máy-đến-máy (host-to-host) và cổng-tới-cổng (gateway-to-gateway). Trong liên kết máy (host) (đôi khi được gọi là "end-to-end" hay "mút-đến-mút"), các hệ thống gửi và nhận là hai hay nhiều máy chủ, chúng thiết lập kết nối an toàn để truyền tin giữa chúng. Trong liên kết cổng (gateway) (còn được gọi là "subnet-to-subnet" hay "mạng con-tới-mạng con"), các hệ thống nhận và gửi là những cổng an ninh, chúng thiết lập kết nối tới các hệ thống ngoài (không tin cậy) thay mặt cho những trạm tin cậy được kết thành những mạng con (tin cậy) bên trong. Các mạng con tin cậy được định nghĩa như một kênh truyền tin (ví dụ như Ethernet) chứa một hay nhiều trạm tin cậy lẫn nhau không tham gia vào các tấn công chủ động hay bị động. Liên kết cổng-tới-cổng thường được xem như một đường hầm (tunnel) hay mạng riêng ảo (Virtual Private Network-VPN). Dạng thứ ba, máy-tới-mạng con cũng có thể được. Trong trường hợp này, cổng an ninh được sử dụng để thiết lập kết nối giữa các máy ở ngoài và các trạm tin cậy ở các mạng trong. Dạng này đặc biệt hữu ích cho những nhân viên lưu động hay những người dùng vé tháng, họ cần truy nhập ứng dụng và dữ liệu trong các hệ thống trong thông qua mạng không tin cậy, giống như Internet.

### *2.4 Quản lý khóa*

Khả năng quản lý và phân phối hiệu quả khóa mã là vô cùng quan trọng đối với thành công của một hệ thống mật mã bất kỳ. Kiến trúc bảo mật IP bao gồm lược đồ quản lý khóa tầng ứng dụng, nó hỗ trợ các hệ thống dựa trên khóa công khai và khóa bí mật, cũng như phân phối khóa tự động hay thủ công. Nó cũng hỗ trợ việc phân phối các tham số phiên cơ bản khác. Việc chuẩn hóa những chức năng này làm cho nó có thể sử dụng được và quản trị các chức năng bảo mật IP trải trên nhiều lĩnh vực bảo mật và nhiều người bán.

Hai đặc tính chính khác của kiến trúc bảo mật IP là hỗ trợ các hệ thống có an ninh nhiều tầng (Multi-Level Security ) và việc sử dụng IANA (Internet Assigned Numbers Authority) để gán các con số cho tất cả các dạng mã IPSEC chuẩn.

## 3- Cài đặt và các cấu trúc

Kiến trúc bảo mật IPSEC xoay quanh 2 cấu trúc IP header, đó là Authentication Header (AH) và Encapsulation Security Payload (ESP). Để hiểu được đầy đủ các cơ chế này hoạt động thế nào, trước hết cần điểm tới khái niệm về tổ hợp bảo vệ (security association). Để đạt tới sự độc lập thuật toán, cách thức mềm dẻo để chỉ ra các tham số phiên được thiết lập. SA trở thành cách thức.

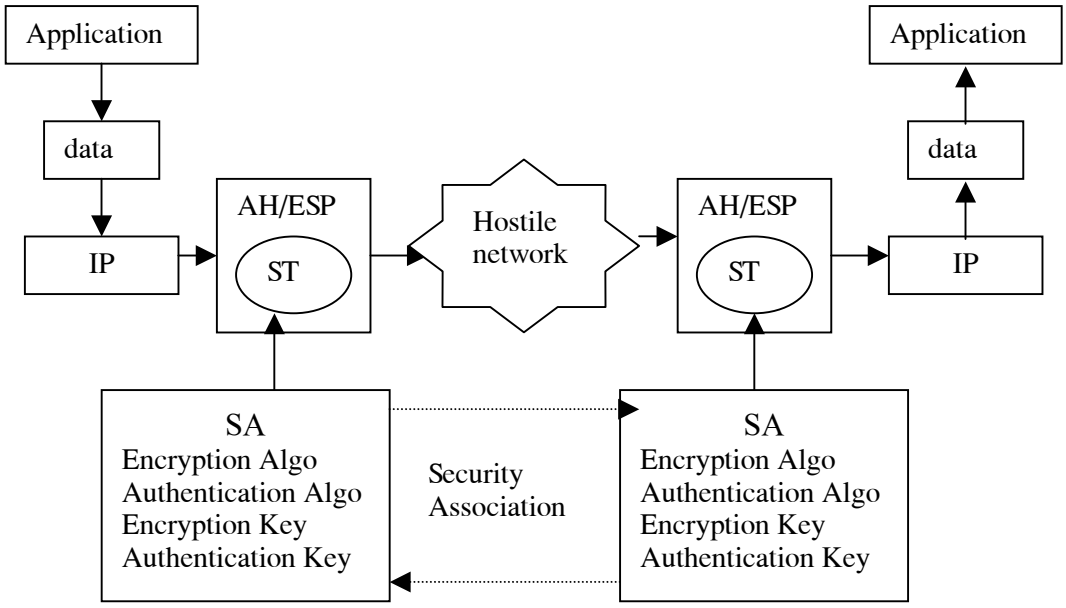
### *3.1 Security Associations (SA)*

Tổ hợp bảo vệ là một bảng hay một bản ghi CSDL bao gồm tập các tham số bí mật chỉ đạo các thao tác bảo mật trên một hay nhiều kết nối mạng. Tổ hợp bảo vệ là một phần của lược đồ khởi tạo một chiều đã nói tới ở trên. Các bảng SA được thiết lập ở các trạm nhận và được chỉ tới ở các trạm gửi bằng tham số chỉ số được biết đến như là Security Parameters Index (SPI). Các thành phần chung nhất trong SA là:

- Kiểu và chế độ hoạt động của biến đổi (transform), ví dụ như DES trong chế độ chuỗi khối. Điều này yêu cầu các tham số. IPSEC được thiết kế độc lập với biến đổi vì thế thông tin này phải được đồng bộ giữa các điểm cuối khi có dữ liệu truyền đi.
- Khoá hoặc các khoá sử dụng bởi thuật toán biến đổi. Theo nguyên nhân dễ hiểu, đó cũng là các tham số bắt buộc. Nguồn khoá có nhiều dạng. Chúng có thể được đưa vào thủ công khi các tổ hợp bảo vệ được định nghĩa trên máy hoặc máy cổng dẫn đường. Chúng có thể được cung cấp thông qua hệ thống phân phối khoá hoặc trong trường hợp hệ mật không đối xứng thì khoá công khai được gửi đi trên đường truyền trong khi kết nối được thiết lập.
- Sự đồng bộ thuật toán mã hoá hoặc véc tơ khởi điểm (initialization vector). Một số thuật toán mã hoá, đặc biệt là đối với những thuật toán dùng chế độ chuỗi, cần phải cung cấp cho hệ thống nhận một khối dữ liệu khởi tạo để đồng bộ thứ tự mã. Thông thường, khối dữ liệu mã hoá đầu tiên phục vụ cho mục đích này, nhưng tham số này cho phép các cài đặt khác. Tham số này được yêu cầu đối với mọi cài đặt ESP, nhưng có thể vắng mặt nếu sự đồng bộ hoá là không được yêu cầu.
- Khoảng thời gian tồn tại của khoá biến đổi. Tham số có thể được định nghĩa bằng khoảng thời gian hoặc tại một thời điểm xác định thì xảy ra việc trao đổi khóa. Không có sự xác định trước về khoảng thời gian cho khoá mật mã. Khoảng mà khoá được biến đổi phụ thuộc vào các thành phần an toàn tại các điểm cuối. Hơn thế nữa tham số này chỉ được gợi ý chứ không phải bắt buộc.
- Thời gian tồn tại của tổ hợp bảo vệ. Không có sự xác định trước nào đối với khoảng thời gian tồn tại của tổ hợp bảo vệ. Độ dài thời gian mà tổ hợp bảo vệ còn có tác dụng phụ thuộc vào sự xác định của các thành phần tại điểm cuối. Tham số này chỉ được gợi ý, không phải bắt buộc.

- Địa chỉ nguồn của tổ hợp bảo vệ. Một tổ hợp bảo vệ thường được thành lập chỉ theo một chiều. Một phiên giao tiếp giữa hai điểm cuối thường sẽ kéo theo hai tổ hợp bảo vệ. Khi mà có nhiều máy gửi đi sử dụng tổ hợp bảo vệ này, tham số có thể được đặt với giá trị có vị trí thay thế (wild-card). Thông thường địa chỉ này giống như địa chỉ nguồn trong phần IP header; tham số này chỉ gợi ý, không phải là bắt buộc.
- Mức nhạy cảm của dữ liệu bảo vệ. Tham số này được yêu cầu đối với các máy  cài đặt nhiều mức an toàn và gợi ý đối với tất cả hệ thống khác. Tham số cung cấp phương thức gán nhãn bảo mật (ví dụ như Secret, Confidential, Unclassified) để đảm bảo định tuyến và xử lý đúng bởi các điểm cuối.

Các tổ hợp bảo vệ thường được thiết lập chỉ trên một chiều. Trước khi một phiên trao đổi an toàn có thể được thành lập thì tổ hợp bảo vệ phải được thành lập ở máy gửi và máy nhận. Những tổ hợp bảo vệ này có thể được cấu hình thủ công hay tự động thông qua giao thức quản lý khoá. Khi một gói dữ liệu được gửi đi cho một máy nhận (có bảo mật), hệ thống gửi sẽ tìm kiếm tổ hợp bảo vệ tương ứng và chuyển giá trị kết quả tới máy nhận. Máy nhận sẽ sử dụng SPI và địa chỉ đích để tìm kiếm tổ hợp bảo vệ trên hệ thống của nó. Trong trường hợp nhiều mức an toàn, nhãn an toàn cũng trở thành một thành phần của tiến trình lựa chọn tổ hợp bảo vệ tương ứng. Hệ thống nhận sẽ dùng các tham số của tổ hợp bảo vệ để xử  lý chuỗi gói tin nhận được từ máy gửi. Để thành lập phiên giao tiếp xác thực đầy đủ thì máy gửi và máy nhận phải tráo đổi vai trò và thiết lập một SA thứ hai theo chiều ngược lại.




Thiết lập SA

Một ưu điểm của lược đồ lựa chọn SA một chiều là hỗ trợ cho kiểu truyền thông broadcast. Các tổ hợp bảo vệ có thể vẫn được thành lập trong chế độ chỉ nhận bằng cách máy nhận chọn lấy một SPI. Gói tin unicast có thể gán một giá trị SPI duy nhất, còn các gói tin multicast có thể gán giá trị SPI cho mỗi nhóm multicast. Tuy nhiên, sự sử dụng của IPSEC đối với kiểu truyền thông broadcast có một số giới hạn. Trình quản lý khoá và phân bố khó khăn, và giá trị của mật mã bị giảm đi bởi vì nguồn của gói tin không được thành lập một cách rõ ràng.

### *3.2 Security Parameters Index (SPI)*

SPI là một số giả ngẫu nhiên 32 bít được sử dụng để xác định duy nhất một tổ hợp an toàn (SA). Nguồn gốc của SPI rất đa dạng. Chúng có thể được đưa vào một cách thủ công khi SA được xác định trên máy hoặc cổng dẫn đường, hoặc chúng được cung cấp thông qua hệ thống phân bố SA. Hiển nhiên, để chức năng an toàn hoạt động đúng, các SPI phải được đồng bộ giữa các điểm cuối. Giá trị SPI từ 1-255 được IANA dành để sử dụng cho các cài đặt trong tương lai. SPI yêu cầu sự quản lý tối thiểu nhưng một số phòng ngừa có thể được đặt trước để chắc chắn rằng giá trị SPI đã được gán không được sử dụng lại quá nhanh chóng sau khi SA tương ứng bị xoá. Giá trị SPI bằng 0 chỉ ra không có một tổ hợp bảo vệ nào tồn tại cho phiên tương tác này. Trên liên kết mút-tới-mút, SPI được sử dụng bởi máy nhận để tìm kiếm tổ hợp bảo vệ. Trên kết nối theo kiểu gateway-to-gateway, unicast, hoặc multicast, hệ thống nhận kết hợp SPI với địa chỉ đích (và trong hệ thống có nhiều mức an toàn, với nhãn an toàn) để xác định SA phù hợp. Bây giờ

chúng ta sẽ xem xét chức năng chứng thực và bảo mật sử dụng SA và SPI như thế nào.

### *3.3 Hàm xác thực (Authentication Function)*

Xác thực IPSEC sử dụng hàm băm mật mã để cung cấp tính toàn vẹn và xác thực mạnh cho gói dữ liệu IP. Thuật toán ngầm định là Message Digest version 5 (MD5), nó không cung cấp dịch vụ chống chối bỏ. Nonrepudiation có thể được cung cấp bởi sử dụng thuật toán mật mã mà hỗ trợ nó (ví dụ RSA). Hàm xác thực IPSEC không cung cấp khả năng bảo mật hoặc chống lại sự phân tích đường truyền.

Hàm được tính toán tên toàn bộ gói dữ liệu sử dụng thuật toán và khoá được chỉ ra trong tổ hợp bảo vệ (SA). Sự tính toán thực hiện trước khi phân đoạn, và các trường có thể biến đổi trong khi truyền, (ví dụ ttl hoặc hop count) bị loại trừ. Dữ liệu xác thực được đặt vào phần Authentication Header (AH) cùng với Security Parameter Index (SPI) được gán cho SA đó. Đặt phần dữ liệu xác thực vào cấu trúc payload (AH) thay cho việc thêm nó vào phần dữ liệu gốc có nghĩa là gói tin người sử dụng vẫn giữ nguyên định dạng và có thể được đọc và xử lý bởi hệ thống không tham gia vào việc xác thực. Hiển nhiên là không có tính bảo mật, và cũng không cần thiết phải thay đổi hạ tầng Internet để hỗ trợ hàm xác thực IPSEC. Các hệ thống không có phần xác thực vẫn xử lý gói tin một cách bình thường.

Phần xác thực authentication header (AH) được chèn vào gói tin sau phần IP header đối với IPv4 và sau phần hop-by-hop header đối với IPv6, đồng thời trước phần ESP header khi sử dụng với hàm bảo mật.

| | | |
|---|---|---|
| Ipv4 Header | AH Header | Upper Protocol ( TCP, UDP) |

Kiểu header được IANA gán cho số 51 và được chỉ ra trong trường next header hoặc trường protocol của cấu trúc header trước đó. Có 5 trường tham số trong một authentication header, 4 trong số chúng hiện tại được dùng:

- Trường next header - được sử dụng để xác định giao thức IP được dùng trong cấu trúc header tiếp theo (do IANA) gán.
- Trường payload length – là số của các word 32-bit chứa trong trường dữ liệu xác thực.
- Trường reserved – dùng cho sự mở rộng trong tương lai. Trường này hiện tại đặt giá trị 0.
- Trường SPI – giá trị duy nhất xác định tổ hợp bảo vệ (SA) sử dụng cho gói tin này.
- Trường authentication data – dữ liệu đầu ra của hàm băm được nối thêm cho thành bội của 32 bit.

| Next Header | Length | RESERVED |
|---|---|---|
| Security Parameter Index | | |
| Authentication Data (variable number of 32-bit words) | | |

Trên hệ thống IP version 4 có hỗ trợ AH cần phải cài đặt IP Authentication Header ít nhất với thuật toán MD5 sử dụng 128-bit khoá. Việc cài đặt AH là bắt buộc với IP version 6 và cũng cần hỗ trợ thuật toán MD5 với 128-bit khoá. Mọi cài đặt AH có tuỳ chọn để hỗ trợ các thuật toán xác thực khác (ví dụ như SHA1). Mặt yếu kém của MD5 (xem Hans Dobbertin, Cryptanalysis of MD5 Compress) sẽ dẫn đến việc thay thế nó trong hoạch định của phiên bản AH tiếp theo. Sự thay thế đó là HMAC-MD5. HMAC là một phương pháp nâng cao cho việc tính toán Hashed Message Authentication Codes mà nó có tính mật mã mạnh hơn. Bởi vì HMAC là một sự nâng cấp chứ không phải sự thay thế, nên nó có thể được dễ dàng thêm vào các cài đặt AH mà không làm ảnh hưởng nhiều đến hệ thống đã có sẵn. Các hệ thống dùng MLS yêu cầu thành lập AH trên gói tin có chứa nhãn nhạy cảm để xác định tính bảo mật mút-tới-mút của các nhãn đó.

Sự tính toán của dữ liệu băm xác thực bởi hệ thống sử dụng Authentication Header không làm tăng đáng kể sức lực tính toán và độ trễ truyền thông; tuy nhiên, sự tác động này được coi là thấp hơn hệ thống mật mã khoá bí mật. Hàm AH đòi hỏi giá cài đặt thấp và dễ xuất khẩu bởi vì nó dựa trên thuật toán băm. Tuy nhiên, có cũng có ý nghĩa làm tăng đáng kể tính an toàn đối với hầu hết phiên truyền thông Internet.

### *3.4 Hàm bảo mật*

Bảo mật IPSEC sử dụng mật mã có khóa để cung cấp tính toàn vẹn và bảo mật của gói tin IP. Thuật toán ngầm định sử dụng chuẩn mã dữ liệu của Mỹ theo chế độ Cipher Block Chain (DES CBC), nó không cung cấp xác thực và chống chối bỏ. Nó có thể cung cấp dịch vụ xác thực bằng cách sử dụng biến đổi mật mã hỗ trợ nó. Tuy nhiên, một sự gợi ý là nếu cần xác thực hoặc chống chối bỏ thì hãy sử dụng IP Authentication Header. Hàm bảo mật IPSEC không cung cấp bảo vệ chống kiểu tấn công phân tích truyền thông.

Có hai kiểu hoạt động, tunnel và transport. Trong chế độ tunnel thì toàn bộ nội dung của gói tin IP nguyên bản được bọc bằng ESP (Encapsulation Security Payload) sử dụng thuật toán và khoá xác định trong SA. Kết quả phần mã hoá ESP cùng với SPI được xác định bởi SA trở thành phần dữ liệu của gói thứ hai đi sau IP header ở dạng rõ. Phần đầu rõ này thường được lặp đúp với phần đầu của gói tin IP nguyên bản đối với sự truyền thông giữa máy-tới-máy, nhưng trong việc bảo mật giữa hai getway thì phần đầu rõ này là địa chỉ của các getway, trong khi phần header được mã hoá chỉ rõ máy cuối nào trong mạng nội bộ bên kia (địa chỉ đến thực sự). Trong chế độ transport thì chỉ có các phần ở tầng transport (ví dụ, TCP, UDP) được đóng viên trong ESP, vì thế phần IP header rõ sẽ lấy IP header

nguyên bản của gói tin đó. Mặc dù thuật ngữ "transport" dường như chỉ giới hạn trong ở giao thức TCP và UDP, điều đó không đúng. Chế độ transport ESP hỗ trợ tất cả các giao thức IP. Trình xử lý cả hai chế độ thực hiện trước khi xảy ra phân đoạn ở đầu ra và sau khi hợp lại ở đầu vào.

ESP header được chèn vào gói tin bất cứ chỗ nào sau IP header và trước giao thức ở tầng vận chuyển. Nó phải xuất hiện sau AH header khi chúng ta sử dụng nó với hàm xác thực.

| | | |
|---|---|---|
| Ipv4 Header | AH Header (optional) | Encapsulated Security Payload |

Kiểu header được IANA đặt số là 50 và tương tự như trường next header hoặc trường giao thức của cấu trúc header trước đó. Phần ESP header chứa 3 trường:

- Trường SPI – là định danh duy nhất cho SP sử dụng để xử lý gói tin này. Trường này là trường bắt buộc trong trường ESP.
- Trường opaque transform data – Tham số thêm được yêu cầu để hỗ trợ biến đổi mật mã sử dụng SA này (ví dụ như véc tơ khởi điểm). Dữ liệu chứa trong trường này phụ thuộc vào phép biến đổi và có độ dài thay đổi. IPSEC chỉ yêu cầu nó được thêm vào sao cho có độ dài là bội của 32-bit.
- Trường dữ liệu mã hoá – dữ liệu đầu ra của trình biến đổi mật mã.

| | | |
|---|---|---|
| Security Parameter Index | | |
| Initialization Vector Data (variable number of 32-bit words) | | |
| Payload Data (variable length) | | |
| . . . Padding Data | Pad Length | Payload type |

IP phiên bản 4 hoặc phiên bản 6 có hỗ trợ ESP phải cài đặt DES CBC. Tất cả các cài đặt của ESP đều có tuỳ chọn để hỗ trợ các thuật toán mã hoá khác. Ví dụ, nếu không có một tổ hợp bảo vệ nào thích hợp cho gói dữ liệu đến (ví dụ người nhận không có khoá), người nhận phải bỏ phần mã hoá ESP và ghi lại lỗi trên hệ thống. Các giá trị được khuyến cáo nên ghi lại đó là giá trị SPI, ngày/thời gian, địa chỉ nơi gửi và nơi nhận, và định danh luồng ID. Phần ghi lại (log) có thể bao gồm các dữ liệu đặc thù riêng của phép cài đặt. Một sự gợi ý rằng hệ thống nhận không nên gửi ngay phản hồi về lỗi tới hệ thống gửi ngay tức thì bởi vì đây là điểm để dễ dàng khai thác tấn công kiểu từ chối dịch vụ.

Sự tính toán dữ liệu mã hoá bởi hệ thống sử dụng ESP làm gia tăng khối lượng xử lý và thời gian trễ truyền thông. Toàn bộ tác động phụ thuộc vào thuật toán mã hoá và cách cài đặt. Thuật toán mã hoá với khoá bí mật yêu cầu ít thời gian xử lý hơn thuật toán mã hoá với khoá công khai, và các cài đặt dựa trên phần cứng dường như nhanh hơn và ít ảnh hưởng đến hệ thống.

Chức năng ESP (Encapsulation Security Payload) khó cài đặt hơn và là đối tượng của một số hạn chế sử dụng cũng như xuất khẩu quốc tế, nhưng cấu trúc mềm dẻo của nó, các khả năng VPN và tính bảo mật mạnh là lý tưởng cho công việc làm ăn cần một môi trường truyền thông an toàn trên mạng Internet.

### *3.5 Quản lý khóa*

Chức năng quản lý khoá bao gồm sinh, xác thực, và phân phối khoá mật mã được yêu cầu để thiết lập đường truyền bí mật. Chức năng thường gắn chặt vào thuật toán mật mã mà chúng hỗ trợ, nhưng cái chung, việc sinh khoá (generation) là chức năng dùng để tạo ra khoá và quản lý thời gian sống của chúng và cách sử dụng; xác thực là tiến trình sử dụng để xác nhận chính xác máy hoặc getway (cổng dẫn đường) yêu cầu dịch vụ khoá; và phân phối là quá trình dùng để chuyển khoá tới hệ thống yêu cầu theo một phương thức an toàn.

Có hai cách tiếp cận để trao đổi khoá IP, host-oriented (theo hướng máy) và user-oriented (theo hướng người dùng). Khoá theo kiểu host-oriented là mọi người dùng chia sẻ cùng một khoá khi mà dữ liệu truyền đi giữa các điểm cuối (ví dụ, host và gateway). Khoá theo kiểu user-oriented được thành lập với mỗi khoá riêng cho mỗi phiên liên lạc người dùng mà nó truyền dữ liệu giữa các điểm cuối. Các khoá không được dùng chung giữa các người dùng hoặc các ứng dụng. Người dùng có các khoá khác nhau cho các phiên Telnet hoặc FTP. Hệ thống với nhiều mức an toàn (MLS) yêu cầu khoá theo kiểu hướng người dùng để bảo mật giữa các mức khác nhau. Nhưng cũng không phải là bất bình thường khi hệ thông không phải là đa mức an toàn có người dùng, nhóm, hoặc các tiến trình mà không tin tưởng lẫn nhau. Hơn thế nữa, IETF Security Working Group gợi ý là nên dùng khoá theo kiểu định hướng người dùng đối với tất cả các cài đặt quản lý khoá IPSEC.

Ở đây chúng ta chỉ để cập đến trình quản lý khoá mật mã theo kiểu truyền thống. Tuy nhiên, các chức năng quản lý khoá theo kiểu truyền thống không có khả năng hỗ trợ IPSEC một cách đầy đủ. Sự độc lập biến đổi IPSEC yêu cầu tất cả các thành phần của tổ hợp bảo vệ, không chỉ riêng khoá mật mã, được phân phối đến được điểm cuối. Nếu không đủ tham số của tổ hợp bảo vệ, các điểm cuối sẽ không thể xác định được khoá mật mã đã được áp dụng như thế nào. Điều này dẫn đến cần phát triển Internet Security Association and Key Management Protocol (ISAKMP). ISAKMP hỗ trợ chức năng quản lý khoá chuẩn và bao gồm các thành phần để bắt tay, thành lập, sửa đổi, và xoá các tổ hợp bảo vệ và thuộc tính của chúng. Ở phần còn lại của phần này chúng ta sử dụng thuật ngữ quản lý SA để chỉ ra trình quản lý toàn bộ cấu trúc SA (bao gồm cả khoá mật mã) và thuật ngữ quản lý khoá để chỉ đến các tham số khoá cho một SA. Một điều quan trọng để lưu ý khác cần phải ghi nhớ là quản lý khoá có thể thực hiện riêng biệt với trình quản lý SA. Ví dụ, trao đổi khoá theo hướng host-oriented sử dụng trình quản lý SA để thành lập cả tham số phiên làm việc và khoá mật mã, trong khi đó trao đổi

khoá theo hướng user-oriented  sử dụng chức năng quản lý SA để thành lập tham số khởi tạo phiên làm việc và chức năng quản lý khoá để cung cấp mỗi khoá phiên được dùng.

Kiểu đơn giản nhất để quản lý SA cũng như quản lý khoá là quản lý thủ công. Người quản trị an toàn hệ thống thường nhập vào tham số SA và khoá mã hoá cho các hệ thống của họ và các hệ thống mà nó giao tiếp với. Tất cả các cài đặt Ipv4 và Ipv6 của IPSEC đều yêu cầu hỗ trợ cấu hình thủ công đối với tổ hợp bảo vệ và khoá. Cấu hình thủ công hoạt động tốt với phạm vi hẹp, môi trường tĩnh không có sự biến đổi nhưng nó rất khó khăn để điều chỉnh cho môi trường rộng, đặc biệt nếu bao gồm việc quản trị nhiều vùng. Trong những môi trường như vậy chức năng quản lý SA và khoá phải được tự động. Vì lý do này mà chức năng ISAKMP được thiết kế.

### *3.6 Internet Security Association and Key Management Protocol (Tổ hợp bảo vệ Internet và Giao thức quản lý khóa)*

Giao thức ISAKMP cung cấp một phương thức chuẩn, mềm dẻo và có khả năng mở rộng để phân phối các tổ hợp bảo vệ và các khóa mật mã.  Giao thức định nghĩa các thủ tục để xác thực người đối thoại, tạo và quản lý các tổ hợp bảo vệ, các kỹ thuật để sinh và quản lý khóa cũng như các tổ hợp bảo vệ, và cách để giảm nhẹ các nguy cơ như tấn công lặp lại hay tấn công từ chối dịch vụ. ISAKMP đã được thiết kế để hỗ trợ các dịch vụ AH và ESP, nhưng nó còn đi xa hơn nữa. ISAKMP có khả năng hỗ trợ các dịch vụ bảo mật tại các tầng vận chuyển và tầng ứng dụng cho rất nhiều cơ chế an toàn khác. Điều đó có thể là do ISAKMP phân tách chức năng quản lý tổ hợp bảo vệ khỏi cơ chế trao đổi khóa. ISAKMP có giao thức trao đổi khóa độc lập. Nó cung cấp một qui định chung để thỏa thuận, trao đổi, sửa đổi và xóa bỏ các tổ hợp bảo vệ giữa các hệ thống không giống nhau. Việc tập trung hóa cách quản lý các tổ hợp bảo vệ bằng ISAKMP làm giảm nhiều chức năng trùng lặp trong mỗi giao thức bảo mật và giảm đáng kể thời gian thiết lập kết nối bởi vì ISAKMP có thể thỏa thuận một lần cho một tập các dịch vụ.

Việc bàn luận chi tiết về ISAKMP vượt ra ngoài khuôn khổ của bài viết này cho nên chúng tôi chỉ đề cập đến các thao tác và yêu cầu chức năng của tổ hợp bảo vệ và hệ thống quản lý khóa. Tổ hợp bảo vệ và hệ thống quản lý khóa là ứng dụng dịch vụ điều đình giữa các hệ thống thiết lập liên kết mật. Nó không tham gia tích cực trong việc truyền dữ liệu giữa các hệ thống này. Nó chỉ hỗ trợ việc thiết lập mói liên kết mật bằng cách sinh, xác thực, và phân phối các tổ hợp bảo vệ cũng như khóa mật mã được yêu cầu.

Hai tham số cần phải thỏa thuận để hệ thống hoạt động đúng. Thứ nhất, một quan hệ tin cậy cần phải thiết lập giữa các hệ thống đầu cuối và người quản lý SA. Người quản lý SA có thể là hệ thống thứ ba, giống như trung tâm phân phối khóa

KERBEROS (Key Distribution Center-KDC)- hoặc tích hợp vào cài đặt IPSEC tại đầu cuối. Mỗi giải pháp yêu cầu thiết lập bằng tay SA cho mỗi người quản trị và các đầu cuối mà người quản trị liên lạc với. Ưu điểm là một số ít SA làm bằng tay có thể được sử dụng để thiết lập vô số các kết nối bảo mật. Một số nhà bán hàng đã chọn cách tích hợp ISAKMP vào các hệ thống đầu cuối và sử dụng hệ thống thứ ba (Certificate Authority- Nhà chức trách chứng thực) để kiểm chứng quan hệ tin cậy lúc đầu. Yêu cầu thứ hai đối với các điểm cuối là phải có một đối tượng thứ ba tin cậy chung. Nói một cách khác, cả 2 điểm cuối cần phải có hệ thống quản lý SA hay nhà chức trách chứng thực mà cả hai cùng tin cậy.

Thao tác là khá dễ hiểu. Chúng ta sẽ sử dụng các hệ thống có tích hợp các SA cho màn diễn này. Hệ thống A muốn thiết lập phiên liên lạc mật với Hệ thống B nhưng hiên tại không có một tổ hợp bảo vệ hợp lệ nào tồn tại giữa chúng. Hệ thống A liên lạc với chức năng quản lý SA trên Hệ thống B. Quá trình sẽ được làm ngược lại (nhớ rằng các SA chỉ được thiết lập theo một chiều) khi Hệ thống B thiết lập đường đi quay lại mật tới Hệ thống A. ISAKMP có khả năng thỏa thuận SA hai chiều trong một lần tương tác cho nên việc thỏa thuận đường đi quay lại riêng biệt thường là không cần.

Giao thức ISAKMP có 4 thành phần chức năng chính sau. Đó là:

- Xác thực người đối thoại
- Thiết lập và quản lý khóa mật mã
- Tạo và quản lý tổ hợp bảo vệ.
- Giảm mối đe dọa.

Xác thực thực thể tại đầu bên kia của mối liên lạc là bước đầu tiên để thiết lập phiên liên lạc an toàn. Không có việc xác thực thì không thể tin cậy vào nhận diện của thực thể và việc thiếu nhận diện hợp lệ làm cho việc kiểm sóat truy nhập vô nghĩa. Có lợi ích gì khi liên lạc mật với một hệ thống không tin tưởng?

ISAKMP qui định việc sử dụng chữ ký số khóa công khai (như DSS, RSA) để thiết lập một xác thực mạnh cho tất cả các trao đổi ISAKMP. Chuẩn không chỉ ra cụ thể thuật toán nào. Mật mã khóa công khai tỏ ra hiệu quả, mềm dẻo để phân phối các bí mật chung và các khóa phiên. Tuy vậy, để hoàn toàn hiệu quả cần phải có cách liên kết giữa khóa công khai và từng thực thể cụ thể. Trong các ứng dụng lớn, chức năng này được cung cấp bởi một người tin cậy thứ ba (trusted third party-TTP) giống như nhà chức trách chứng thự (CA). Các ứng dụng nhỏ có thể chọn việc sử dụng các khóa được thiết đặt bằng tay. ISAKMP không định ra các giao thức được sử dụng để liên lạc với người tin cậy thứ ba.

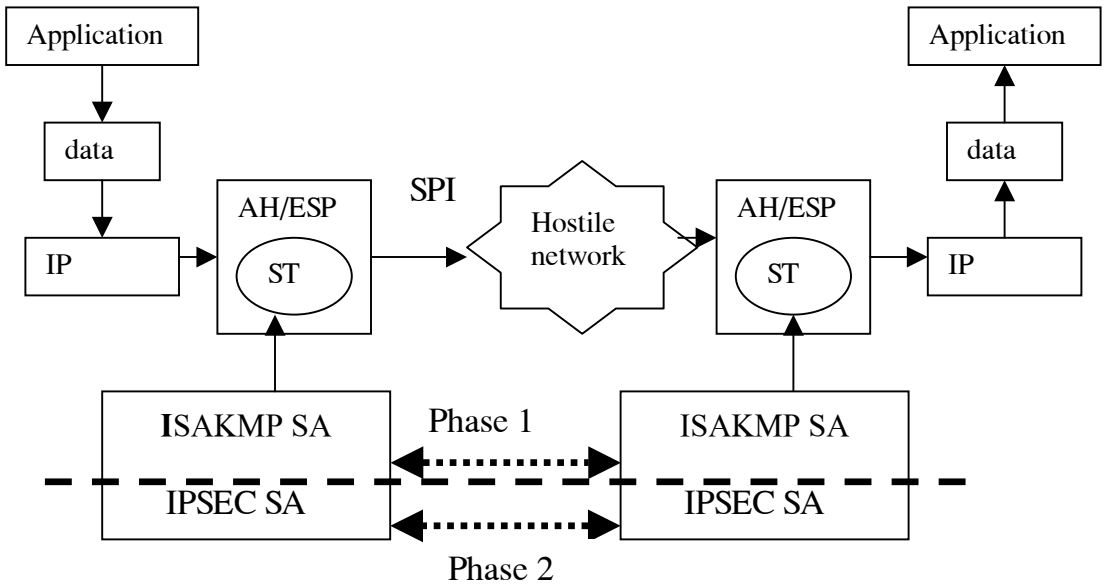
Việc thiết lập khóa bao gồm việc sinh các khóa ngẫu nhiên và vận chuyển các khóa này tới các bên tham gia. Trong hệ mật khóa công khai RSA việc vận chuyển khóa được thực hiện bằng cách mã khóa phiên bằng khóa công khai của

người nhận. Khóa phiên đã được mã hóa khi đó được gửi tới người nhận, người này giải mã nó bằng khóa bí mật. Trong hệ thống Diffie-Hellman thì khóa công khai của người nhận cần kết hợp với thông tin khóa bí mật của người gửi để tạo ra khóa bí mật chung. Khóa này có thể được sử dụng như là khóa phiên hoặc để vận chuyển một khóa phiên thứ hai được sinh ngẫu nhiên. Trong ISAKMP, những trao đổi khóa này được thực hiện có sử dụng xác thực mạnh. ISAKMP không định ra giao thức trao đổi khóa cụ thể, nhưng đã xuất hiện rằng Oakley sẽ trở thành chuẩn.

Việc sinh và quản lý tổ hợp bảo vệ bao gồm 2 pha của thỏa thuận kết nối. Pha thứ nhất thiết lập tổ hợp bảo vệ giữa các người quản trị SA ở hai đầu cuối. Pha thứ hai thiết lập các tổ hợp bảo vệ cho giao thức bảo mật được chọn theo phiên. Pha một tạo lập mối tin tưởng giữa các người quản trị và các đầu cuối; pha thứ hai tạo lập mối tin cậy giữa 2 đầu cuối. Sau khi pha thứ hai được hoàn tất, người quản lý SA không tiếp tục tham gia vào kết nối nữa.

Giao thức ISAKMP tích hợp các cơ chế để chống lại các nguy cơ như từ chối dịch vụ (Denial of Service), chặn bắt (Hijacking) và tấn công người đứng giữa (Man-in-the-Middle). Dịch vụ quản lý gửi trước một thẻ chống cản trở (an ti-clogging token, cookie) tới hệ thống yêu cầu  để thực hiện bất kỳ một thao tác nào tốn nhiều công sức CPU. Nếu người quản trị không nhận được trả lời của thẻ này, nó coi yêu cầu như là không hợp lệ và bỏ yêu cầu đi. Mặc dù đây không là cách bảo vệ chống cản trở tốt nhất, nó đủ hiệu quả để chống lại phần lớn các tấn công làm tắc nghẽn thông thường. Cơ chế chống cản trở cũng rất có lợi để phát hiện tấn công chuyển hướng. Vì nhiều thẻ được gửi đi trong quá trình thiết lập mỗi phiên, nên bất cứ một cố gắng nào nhằm chuyển hướng dòng dữ liệu đến điểm cuối khác sẽ bị phát hiện.

Giao thức ISAKMP liên kết quá trình xác thực và quá trình trao đổi SA/khóa vào một dòng dữ liệu duy nhất. Điều này làm cho những tấn công dựa vào việc chặn bắt và thay đổi dòng dữ liệu (như chặn bắt, người đứng giữa) hoàn toàn vô tác dụng. Mọi sự can thiệp hay sửa đổi dòng dữ liệu sẽ bị phát hiện bởi người quản trị và mọi xử lý tiếp theo bị dừng. ISAKMP cũng áp dụng một máy trạng thái cài đặt sẵn để phát hiện việc xóa bỏ dữ liệu, điều này đảm bảo cho những SA dựa trên những trao đổi một phần sẽ không được thiết lập. Cuối cùng, để chống lại sự đe dọa, ISAKMP định ra việc ghi nhật ký và các yêu cầu cảnh báo đối với tất cả các hành động bất thường và giới hạn việc sử dụng việc thông báo lỗi trên đường truyền.




ISAKMP/Oakley

**4- Dùng IPSEC ở đâu?**

Tất nhiên, các chức năng xác thực và mã hóa dữ liệu trên mạng có thể được cung cấp ở các tầng khác. Nhiều thủ tục bảo mật làm việc ở các tầng phía trên của IP, ví dụ:

- PGP mã hóa và xác thực thư tín
- SSH xác thực việc truy nhập từ xa và mã hóa cả phiên làm việc
- SSL hay TLS (Transport Layer Security) cung cấp bảo mật ở tầng socket, ví dụ cho trình duyệt web an toàn.

Có một số kỹ thuật khác làm việc ở tầng thấp hơn IP. Ví dụ, dữ liệu trong mạch truyền thông hay cả mạng có thể được mã hóa bởi một thiết bị cứng đặc biệt. Đây là một thực tế thường gặp trong các ứng dụng đòi hỏi độ bảo mật cao.

IPSEC gateway có thể cài đặt ở bất kỳ chỗ nào nó được yêu cầu:

- Một cơ quan có thể chọn chỉ cài đặt IPSEC ở các bức tường lửa giữa các mạng LAN và Internet. Điều này cho phép họ tạo ra các mạng riêng ảo liên kết nhiều văn phòng. Điều này bảo vệ chống lại bất cứ ai ở ngoài site của họ.
- Tổ chức khác có thể cài đặt IPSEC tại các máy chủ của các ban, như vậy mọi cái trên mạng xương sống của công ty đều được mã hóa. Điều này bảo vệ thông tin trên mạng với bất kỳ ai, trừ ban nhận và ban gửi.
- Công ty khác có thể ít quan tâm đến việc mã hóa thông tin và chú trọng hơn đến việc kiểm sóat truy nhập vào tài nguyên. Họ có thể dùng việc xác thực gói IPSEC như là một phần của cơ chế kiểm sóat truy nhập, việc xác thực có thể dùng riêng hoặc đồng thời với việc dịch vụ bảo mật của IPSEC

- Hoàn toàn có thể (giả sử có đủ công suất tính toán và IPSEC được cài đặt tại mỗi điểm) là cho mỗi máy trở thành IPSEC gateway của chính mình, như vậy mọi cái trên mạng LAN đều được mã hóa.
- Các kỹ thuật trên có thể tổ hợp với nhau theo nhiều cách. Một công ty có thể yêu cầu việc xác thực ở mọi nơi trên mạng trong khi chỉ sử dụng mã hóa tại một số đường.

**5- Ưu điểm của IPSEC**

Có một số ưu điểm mà IPSEC có so với việc bảo mật ở các tầng khác. IPSEC là cách tổng quát nhất để cung cấp các dịch vụ bảo mật trên Internet.

- Các dịch vụ ở tầng cao hơn chỉ bảo vệ một giao thức, ví dụ PGP chỉ bảo mật cho thư tín
- Các dịch vụ ở tầng thấp hơn chỉ bảo vệ một môi trường (medium); ví dụ như một cặp thiết bị mã tại 2 đầu của một đường truyền nào đó

Trong khi đó IPSEC có thể bảo vệ bất kỳ giao thức nào chạy trên IP và bất kỳ môi trường nào mà IP chạy trên nó. Hơn nữa, nó có thể bảo vệ một tổ hợp của các giao thức ứng dụng chạy trên một tổ hợp phức tạp của môi trường. Đây là tình huống phổ biến trong truyền thông Internet, cho nên chỉ có IPSEC là giải pháp tổng thể.

IPSEC có thể cung cấp một số dịch vụ bảo mật ở mức nền, không ảnh hưởng gì đến người sử dụng. Để sử dụng PGP cho mục đích mã hóa hay xác thực thư tín, ví dụ, người sử dụng ít nhất phải:

- nhớ câu mật khẩu passphrase
- giữ nó bí mật
- tuân theo thủ tục để xác nhận tính hợp lệ của khóa tương ứng

Một số tổ chức có thể có thẻ thông minh hoặc một phương pháp nào đó khác để giải quyết hai yêu cầu đầu và PKI (Public Key Infrastructure) cùng với thư điện tử có thể giải quyết yêu cầu thứ ba, cho nên gánh nặng có thể không đè lên người sử dụng. Nhưng mỗi hệ thống đều có những đòi hỏi nào đó đối với người sử dụng, nên không có hệ thống nào là an toàn nếu người sử dụng tùy tiện trong việc tuân thủ các yêu cầu.

IPSEC là cơ chế chung để bảo mật IP. Trong khi IPSEC không cung cấp tất cả các chức năng của một chương trình bảo mật thư, nó có thể mã hóa thư. Đặc biệt, nó đảm bảo rằng tất cả thư đi giữa 2 hay một nhóm các địa điểm là được mã hóa. Một kẻ tấn công chỉ nhìn vào sự vận tải bên ngoài, không truy nhập vào một cái gì ở trên hay ở sau máy cửa ngõ IPSEC thì không thể đọc được thư. Kẻ tấn công bị che mắt bởi IPSEC giống như là bởi PGP.

Ưu điểm là IPSEC có thể cung cấp cùng một cơ chế bảo vệ cho mọi thứ được truyền qua IP. Ví dụ, trong một mạng công ty, PGP cho phép các văn phòng

chi nhánh có thể trao đổi thư mật với văn phòng trung tâm. SSL và SSH cho phép bạn truy nhập an tòan các trang web, kết nối như một terminal tới máy chủ,...IPSEC có thể hỗ trợ tất cả các ứng dụng đó, thêm vào đó là truy vấn cơ sở dữ liệu, chia sẻ tệp (NFS hay Windows), các thủ tục khác được bọc trong IP (Netware, Apptalk,...), phone-over-IP, video-over-IP, ...anything-over-IP. Hạn chế duy nhất là không hỗ trợ IP Multicast, mặc dù Internet Draft cho nó đã có.

Để sử dụng IPSEC người sử dụng không phải làm một thao tác nào cả, thậm chí họ không cần biết là có nó. Nhưng người quản trị mạng thì cần phải biết và phải tốn công sức để thiết đặt cấu hình.

IPSEC có thể và thường được sử dụng cùng với các thủ tục bảo mật ở các mức khác. Nếu hai điểm cần liên lạc với nhau qua Internet thì IPSEC rõ ràng là cách bảo vệ kênh liên lạc. Nếu hai điểm khác có đường kết nối trực tiếp với nhau thì hoặc mã luồng (link encryption) hoặc IPSEC có thể dùng. Hãy chọn một thứ hay dùng cả hai. Không phụ thuộc vào cái mà bạn dùng tại tầng IP hay bên dưới tầng IP, hãy sử dụng phía trên tầng IP bất cứ cái gì được yêu cầu. Không phụ thuộc vào việc bạn dùng cái gì ở trên tầng IP, IPSEC luôn làm cho việc tấn công vào các tầng ở phía trên IP trở nên khó khăn hơn. Chú ý rằng tấn công man-in-the-middle trong nhiều thủ tục trở nên khó khăn hơn nếu việc xác thực ở mức gói được thực hiện trong kênh truyền.

## 6- Các hạn chế của IPSEC

IPSEC được thiết kế để bảo mật các kết nối IP giữa các máy tính. Nhưng cũng cần nhớ rằng có nhiều cái nó không làm được. Sau đây là một số hạn chế.

- *IPSEC là không an toàn nếu hệ thống của bạn không an toàn*

An toàn hệ thống trên các máy IPSEC gateway là yêu cầu cần thiết để cho IPSEC hoạt động được như đã thiết kế. Không có hệ thống an toàn nếu các máy được sử dụng trong đó (underlying machines) bị phá hoại. Hãy xem các cuốn sách về an toàn của các hệ Unix ví dụ như sách của Garfinkel & Spafford[1] hay các chỉ dẫn web cho Linux security hay các cuốn sách về an toàn máy tính nói chung.

- *IPSEC không bảo mật ở dạng end-to-end*

IPSEC không cung cấp dịch vụ bảo mật end-to-end như các hệ thống hoạt động ở các tầng cao hơn. IPSEC mã hóa liên kết IP giữa 2 máy tính, đây là điều khác với việc mã thư tín giữa 2 người sử dụng hay giữa các ứng dụng.

Ví dụ, nếu bạn cần mã thư tín từ máy tính của người gửi tới máy tính của người nhận và chỉ người nhận giải mã được, có thể sử dụng PGP hay các hệ thống

[1] **Garfinkel & Spafford *Practical Unix Security***
**O'Reilly 1996 ISBN 1-56592-148-8**

tương tự. IPSEC có thể mã một liên kết bất kỳ hoặc tất cả các liên kết giữa 2 máy chủ thư tín, hoặc giữa một máy chủ và các máy trạm. Nó cũng có thể sử dụng để bảo mật liên kết IP trực tiếp (direct IP link) giữa máy của người gửi và máy của người nhận. Cái mà không được đảm bảo là tính bảo mật end-to-end user-to-user. Nếu chỉ có IPSEC được sử dụng để bảo mật thư tín, thì bất kỳ một người sử dụng nào với quyền thích hợp trên một máy bất kỳ nơi thư được lưu trữ (ở hai đầu hoặc tại bất kỳ một máy chủ store-and-forward nào trên đường đi của thư) đều có thể đọc nó.

Thực ra, IPSEC mã các gói tin từ máy bảo mật cửa ngõ khi nó rời khỏi địa điểm (site) của người gửi và giải mã gói tin khi nó đến máy của ngõ của địa điểm người nhận. Điều này cũng không gần với việc cung cấp dịch vụ end-to-end. Đặc biệt, mọi người với quyền thích hợp trong cả hai mạng LAN có thể chặn bắt thư tín ở dạng không mã.

- *IPSEC không làm được tất cả*

IPSEC không thể cung cấp tất cả các chức năng của một hệ thống làm việc ở các tầng cao hơn trong stack thủ tục. Nếu bạn cần tài liệu được ký điện tử bởi một người nào đó, thì bạn cần chữ ký số và hệ mã khóa công khai để kiểm tra.

Tuy nhiên, chú ý rằng, phép xác thực của IPSEC ở tầng truyền thông làm cho nhiều tấn công ở các tầng cao hơn trở nên khó khăn. Đặc biệt, việc xác thực chống lại tấn công man-in-the-midle.

- *IPSEC xác thực máy, chứ không xác thực người sử dụng*

IPSEC sử dụng cơ chế xác thực mạnh để kiểm soát xem bản tin nào đi tới máy tính nào, tuy vậy không có khái niệm về chỉ số người sử dụng, điều này là thiết yếu đối với nhiều cơ chế và chính sách an toàn. Điều đó có nghĩa là cần cẩn thận khi điều chỉnh các cơ chế an toàn đa dạng trong mạng cùng với nhau. Ví dụ, nếu bạn cần kiểm soát xem ai truy nhập cơ sở dữ liệu trên máy chủ, bạn cần có một cơ chế khác, không dựa vào IPSEC. IPSEC có thể kiểm soát máy tính nào được nối vào máy chủ, đảm bảo rằng dữ liệu truyền tới các máy tính này được bảo mật, và chỉ có thế. Hoặc là máy tính cần phải tự kiểm soát việc truy nhập của người sử dụng, hoặc là cần phải có một dạng xác thực người sử dụng theo kiểu cơ sở dữ liệu, không phụ thuộc vào IPSEC.

- *IPSEC không dừng được tấn công từ chối dịch vụ*

Tấn công từ chối dịch vụ nhằm làm cho hệ thống sụp đổ, quá tải hoặc trở nên nhầm lẫn đến mức người sử dụng hợp pháp không truy nhập được dịch vụ mà hệ thống cung cấp. Điều này khác với tấn công trong đó người tấn công muốn sử dụng dịch vụ hoặc làm làm cho dịch vụ hoạt động nhưng cho kết quả sai.

IPSEC làm dịch chuyển nền tảng của các tấn công DoS; các tấn công có thể chống lại một hệ thống đã có IPSEC khác so với các tấn công dùng để chống lại một hệ thống khác. Tuy nhiên, nó không loại trừ được những tấn công dạng này.

- *IPSEC không dừng được các phân tích giao thông mạng*

Phân tích giao thông mạng là cố gắng nhận được tri thức từ các bản tin mà không quan tâm đến nội dung của chúng. Trong trường hợp IPSEC, điều đó có nghĩa là các phân tích dựa trên những gì nhìn thấy ở các header chưa được mã hóa của các gói tin đã mã hóa- địa chỉ máy cổng nguồn hoặc đích, độ dài gói,...

IPSEC không được thiết kế để chống lại điều này. Việc phòng thủ một phần là có thể, một trong số chúng được mô tả dưới đây, nhưng không rõ ràng rằng việc phòng chống tổng thể được cung cấp.

**7- Cách dùng IPSEC**

- *Chỉ sử dụng xác thực*

Trong một số trường hợp, IPSEC có thể chỉ cung cấp dịch vụ xác thực mà không bảo mật. Ví dụ trong các trường hợp sau:

- Dữ liệu là công khai, nhưng có ai đó muốn chắc chắn rằng đã nhận được dữ liệu đúng, ví dụ như từ website.
- Khi mà việc mã hóa là không cần thiết về mặt pháp luật.
- Khi đã sử dụng mật mã mạnh ở những tầng dưới, ví dụ như ở tầng link.
- Khi mật mã mạnh được được sử dụng ở tầng trên so với IP.

- *Mã hóa mà không có xác thực là nguy hiểm*

Thoạt đầu, thủ tục mã hóa ESP không kiểm tra tính toàn vẹn dữ liệu, nó chỉ làm việc mã hóa. Steve Bellovin đã tìm ra nhiều cách để tấn công nếu sử dụng ESP không kèm theo xác thực. Có thể đọc bài báo "Problem areas for the IP Security Protocols" tại địa chỉ www.research.att.com/~smb/papers/badesp.ps. Để có được kết nối an toàn, bạn phải có AH kèm theo ESP. Chính vì vậy mà nhóm làm việc IPSEC đã đưa việc kiểm tra tính toàn vẹn và tính lặp lại trực tiếp vào bên trong ESP.

Hiện nay, bạn có thể sử dụng:

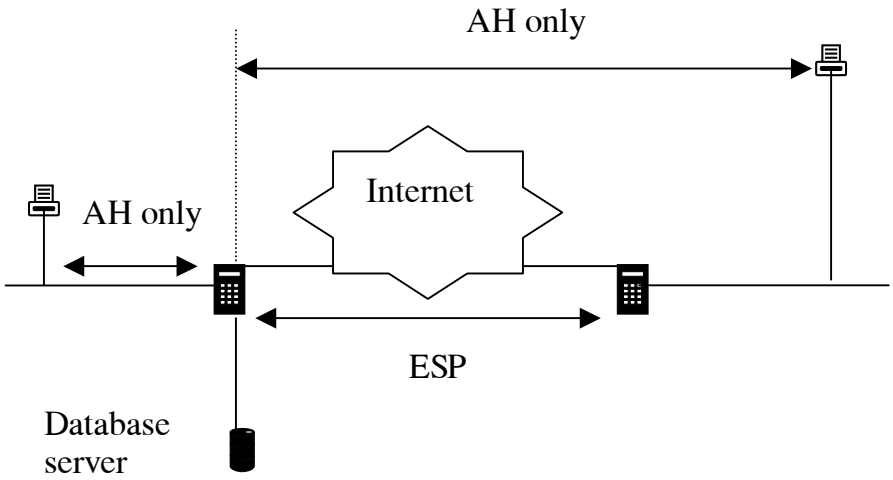
- ESP để bảo mật và xác thực
- AH chỉ riêng cho xác thực.

Một số phương án khác không nên dùng là:

- Mã hóa bằng ESP không có xác thực: như đã được chứng minh bởi Steve Bellovin.
- Mã hóa bằng ESP, xác thực bằng AH: sức tải sẽ lớn hơn so với việc dùng ESP có xác thực.
- Xác thực hai lần, cả bằng AH và ESP: càng chắc chắn

- Dùng ESP có xác thực nhưng không mã hóa: đây chính là dạng ESP "null encryption". Nếu chỉ cần xác thực thì hãy dùng AH.

- ***Xử lý IPSEC nhiều lần là có thể***




Trên đây chúng ta đã mô tả các tổ hợp có thể đối với một kết nối IPSEC. Trong một mạng phức tạp, bạn có thể có nhiều kết nối IPSEC cùng hoạt động. Ví dụ, một kết nối từ máy cá nhân tới máy chủ CSDL yêu cầu AH. Khi làm việc với các máy khác, AH có thể xem như là cái dùng để kiểm tra truy nhập. Bạn có thể quyết định không dùng mã hóa bằng ESP trong mạng cục bộ mà máy chủ đang ở đó. Nhưng đối với một máy trạm ở xa, gói tin đi từ nó đến máy chủ CSDL cần áp dụng AH, vì thế có một đoạn đường gói tin được xử lý IPSEC 2 lần: một lần chỉ có AH (giữa máy trạm và máy cổng), một lần ESP giữa hai máy cổng.

- *Sử dụng mã hóa "không cần thiết" làm thất vọng kẻ tấn công*

Bạn có thể sử dụng mã hóa ngay cả trong trường hợp không bắt buộc để gây khó khăn cho kẻ tấn công. Hãy xét ví dụ: hai văn phòng trao đổi một lượng nhỏ dữ liệu về việc làm ăn và một lượng lớn thông tin Uset news. Thoạt nhìn, chúng ta thấy việc gì phải mã hóa các newsfeed, bởi vì chúng được đăng tải công khai. Nhưng việc mã tất cả bằng cách sử dụng IPSEC sẽ làm cho việc phân tích giao dịch (trafic analysis) trở nên khó khăn hơn.

**8- Kết luận**

Như một chuẩn, IPSEC nhanh chóng trở thành phương pháp được đánh giá cao để bảo mật thông tin trong mạng TCP/IP. Được thiết kế để hỗ trợ nhiều lược đồ mã hóa và xác thực và tính tương giao giữa nhiều người bán hàng, IPSEC có thể được thay đổi để thích hợp với các yêu cầu bảo mật của cả các tổ chức lớn hay nhỏ. Các nền công nghiệp dựa trên công nghệ liên mạng để liên lạc với các đối tác làm ăn sẽ có lợi nhờ vào các lược đồ xác thực và mã hóa mềm dẻo của IPSEC; các

tổ chức lớn sẽ có lợi nhờ tính mở rộng được khả năng quản lý tập trung của IPSEC; mỗi công ty đều có lợi từ khả năng tạo mạng riêng ảo của IPSEC để hỗ trợ những nhân viên làm việc từ xa, nhưng nhân viên hay đi công tác và văn phòng chi nhánh sẽ truy nhập vào công ty qua Internet.

Kiến trúc Giao thức An toàn Internet (Internet Security Protocol Architecture) được thiết kế cùng với những dự kiến trong tương lai, hiện nó đang nhận được sự ủng hộ xứng đáng từ cộng đồng tin học và những người làm công tác bảo mật. Những đánh giá gần đây của những nhà sản xuất lớn như Cisco Systems, cũng như việc thiết lập một chương trình chứng thực hợp tác thông qua Hiệp hội an toàn máy tính thế giới (International Computer Security Association) là dấu hiệu rõ ràng rằng IPSEC đang phát triển trên con đường trở thành chuẩn công nghiệp cho truyền thông giao dịch thương mại trong thế kỷ 21.

## TÀI LIỆU THAM KHẢO


1. An Introduction to IPSEC, Bill Stackpole, Information Security Management Hanbook, 4th edition, Chapter 14, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause, 2000.
2. Tài liệu kèm theo phần mềm FreeS/WAN (http://www.freeswan.org)

# CHƯƠNG 2
# PHÁT HIỆN XÂM NHẬP: LÀM THẾ NÀO ĐỂ TẬN DỤNG MỘT CÔNG NGHỆ VẪN CÒN NON NỚT

Bảo vệ các hệ thống và mạng của mình quả thực là một công việc nan giải. Sự phát triển bùng nổ của Internet cùng với bản chất luôn mở rộng của các mạng khiến cho việc kiểm soát hoàn toàn thích ứng với sự biến đổi gần như là một thách thức không thể vượt qua. Thêm vào đó, công việc bổ sung những điều khiển an toàn thích hợp và vấn đề xảy đến vượt xa dự đoán 20 năm trước đây của các nhà chuyên môn nhìn xa trông rộng nhất. Mặc dầu có những thắng lợi đó đây trong cuộc chiến chống các tội phạm tin học, nhưng thực tế thì lặp lại một sự thật là "không gian điều khiển" thường có một phạm vi quá lớn để có được sự bảo vệ thoả đáng. Tồi tệ hơn nữa, những điều khiển an toàn hôm nay còn làm việc, ngày mai có khả năng sẽ hỏng do nhóm tội phạm triển khai những phương kế mới đánh bại những điều khiển này. Ngoài ra, sự tiếp tục nôn nóng bán phần mềm với nhiều tính năng mới đang dẫn tới việc một phần mềm  thiết kế kém cỏi và thiếu kiểm tra được triển khai ở những vị trí nguy hiểm. Vì thế, có thể việc cài đặt thông thường được dựa vào một phần mềm thiết kế kém cỏi, có lỗi kỹ thuật mà hiện nay những người mới bắt đầu thiết kế sử dụng theo những cách không định trước và tiếp tục chịu sự tấn công từ mọi phía.

Schultz và Wack (SCHU96) đã chỉ rõ rằng các chuyên gia an toàn thông tin cần tránh dựa vào một giải pháp được tin tưởng quá mức trong các kiểm soát an toàn. Xác định những kiểm soát giảm rủi ro hiệu quả nhất theo phạm vi quan hệ vốn-lãi, sau đó cài đặt và duy trì những kiểm soát là một phần thiết yếu của quá trình chế ngự rủi ro. Tuy nhiên, việc đầu tư tất cả các tài nguyên của mình vào việc kiểm soát không phải là sáng suốt vì chiến lược này không dành các tài nguyên cho việc phát hiện và đối phó với các vụ việc ngẫu nhiên liên quan tới an toàn lúc nào cũng có thể xảy ra. Trong phạm vi an toàn thông tin, "tâm lý pháo đài" như vậy (cài đặt rào chắn an toàn nhưng sau đó rào chắn an toàn không làm gì khác cả) không làm việc tốt hơn tý nào so với các lâu đài ở Anh khi những đội quân của Oliver Cromwell chĩa súng đại bác của họ vào chúng. Sẽ tốt hơn rất nhiều nếu sử dụng chiến lược phân tầng, phòng ngự theo chiều sâu bao gồm bảo vệ, kiểm tra và đối phó (cf. Garfinkel and Spafford [GARF96, GARF97]).

Đáng tiếc là sự chấp nhận đơn thuần quan điểm cho rằng quan trọng là đạt được mức độ cân bằng nào đó giữa việc triển khai các kiểm soát và đối phó với các sự cố xảy ra chỉ cải thiện chút ít hiệu quả cho thực tế an toàn thông tin của tổ chức. Một mối nguy hiểm cố hữu khi phải đối phó với sự cố chính là giả thiết ngầm rằng nếu không xuất hiện những sự cố thì tất cả đều tốt. Thoáng qua thì giả thiết này dường như logic. Tuy nhiên, vào năm 1993 và một lần nữa vào năm 1997, các nghiên cứu của Ủy ban bảo vệ các hệ thống thông tin của Mỹ (DISA- Defence

Information Systems Agency) đưa ra những thống kê chứng minh rằng đó là một sai lầm tồi tệ. Van Wyk (VANW94) đã tìm thấy rằng gần 8800 cuộc xâm nhập vào các hệ thống của bộ quốc phòng bởi các đối thủ đáng gờm của DISA, nhưng chỉ một phần sáu bị phát hiện. Chỉ xấp xỉ 4% trong số các cuộc xâm nhập này được báo cáo với người nào đó trong đường dây chỉ huy. Điều này có nghĩa là trong tất cả các cuộc tấn công thành công có ít hơn 1% vừa được cảnh báo và vừa được báo cáo. Ba năm sau, một nghiên cứu tương tự của chính uỷ ban đó đã đưa ra những kết quả gần như giống hệt.

Một điều nữa có thể chỉ rõ là có lẽ nhiều cán bộ của cơ quan bảo vệ không có trình độ hiểu biết kỹ thuật cao như các đồng nghiệp của họ trong ngành kinh doanh vì ngành kinh doanh (theo truyền thống với những mức lương cao hơn của nó) có thể thu hút cán bộ kỹ thuật hàng đầu, đó là người sẵn có khả năng hơn để nhận biết dễ dàng hơn những dấu hiệu của các cuộc tấn công. Do vậy, theo cách lập luận này, trong ngành kinh doanh sẽ có nhiều hơn khả năng ai đó có uy tín về kỹ thuật sẽ cảnh báo về các cuộc xâm nhập xảy ra. Tuy nhiên, lập luận này hoàn toàn chỉ đúng một phần ở nơi mà theo các nghiên cứu của DISA người ta chỉ cố gắng chút ít để che đậy các cuộc xâm nhập ở vị trí trọng yếu. Ngược lại, với những cuộc xâm nhập có thể gọi là "đặc thù hơn", những kẻ tấn công thường dành phần lớn các nỗ lực của họ cho việc giả mạo hành động mà họ đã khởi xướng nhằm tránh bị phát hiện. Điều này được xác nhận thêm nhờ nghiên cứu gần đây nhất của CSI/FBI (POWER99) chỉ ra rằng nhiều công ty không thể xác định được số lượng hay bản chất của các cuộc xâm nhập và những thiệt hại đối với công ty của họ từ các cuộc tấn công vào hệ thống IT, mà trái lại những thiệt hại đó và số lượng các sự cố đang tiếp tục gia tăng.

Điểm chủ yếu ở đây là việc đối phó hiệu quả với vụ việc ngẫu nhiên là quan trọng và cần thiết, nhưng khó làm được bất kỳ điều gì mong muốn nếu mọi người không được cảnh báo về những sự cố xảy ra ở vị trí trọng yếu. Con người cố gắng cảnh báo về những vụ việc ngẫu nhiên, coi như chúng có thể có, trong các trường hợp được giả dụ là không thiếu những cài đặt có thể có hiệu lực hơn. Các chuyên gia an toàn thông tin thường cần nhiều thứ hơn một khả năng chủ động cho phép họ có thể khám phá ra những vụ việc được toan tính hay thực tế đã thành công. Giải pháp là phát hiện xâm nhập. Bài viết này bao trùm chủ đề phát hiện xâm nhập, đề cập tới các kiểu yêu cầu gắn với các hệ thống phát hiện xâm nhập và những cách có thể triển khai cho các hệ thống phát hiện xâm nhập.

## **1-** VỀ PHÁT HIỆN XÂM NHẬP

### **1.1- Phát hiện xâm nhập là gì?**

Phát hiện xâm nhập đề cập tới quá trình khám phá ra việc sử dụng bất hợp pháp các máy tính và mạng thông qua phần mềm được thiết kế nhằm mục đích này. Phần mềm phát hiện xâm nhập có tác dụng đáp ứng chức năng phòng ngừa. Một hệ thống phát hiện xâm nhập hiệu quả vừa phát hiện, vừa báo cáo hành vi bất hợp pháp, chẳng hạn những cố gắng đăng nhập của người nào dó không phải người

dùng hợp pháp hay một cuộc truyền tệp có tính toán và bất hợp pháp tới một hệ thống khác. Phát hiện xâm nhập cũng có thể đáp ứng vai trò trợ giúp đưa ra tư liệu về sự lạm dụng nhằm cung cấp dữ liệu cho việc củng cố các rào chắn hay điều tra nghiên cứu và khởi tố sau khi sự việc xảy ra.

Phát hiện xâm nhập bị đặt tên sai. Như một lĩnh vực, nó bắt đầu với tư cách là một thủ tục phát hiện sự lạm dụng đối với các hệ thống máy tính lớn. Ý tưởng ban đầu ẩn sau các hệ thống phát hiện xâm nhập tự động thường được cho là của James P.Anderson vì bài báo năm 1980 của ông ta về việc sử dụng các file kiểm tra sổ sách thanh toán như thế nào để phát hiện việc sử dụng bất hợp pháp. Thời gian trôi qua, các hệ thống đã trở thành các hệ thống kết nối nhiều hơn thông qua các mạng; sự chú ý đã hướng tới quá trình thâm nhập các hệ thống của "những người ngoài cuộc", vì thế việc bao gồm cả phát hiện "xâm nhập" là một mục tiêu. Trong toàn bộ thảo luận của chúng ta, "phát hiện xâm nhập" có ý nghĩa chung bao hàm việc phát hiện sự lạm dụng của cả người ngoài lẫn người trong nội bộ; những người dùng các hệ thống ID cũng vậy, họ nên giữ ý nghĩ rằng sự lạm dụng của người trong nội bộ cũng phải bị phát hiện.

**1.2- Tại sao dùng tiện ích phát hiện xâm nhập?**

Một giải pháp có khả năng phát hiện xâm nhập sẽ được triển khai tới hàng nghìn cán bộ được huấn luyện đặc biệt để tiếp tục giám sát các hệ thống và các mạng. Giải pháp này thường vẫn không thể thực thi trong hầu hết mọi môi trường vì nó sẽ là phi thực tế. Một vài tổ chức luôn có mong muốn đầu tư ở mức thiết yếu của cải và thời gian đòi hỏi để đào tạo mỗi một "giám sát viên" đạt được trình độ chuyên môn kỹ thuật cần thiết. Việc cho chạy một hay nhiều chương trình tự động được thiết kế một cách hiệu quả để làm cùng một công việc mà không cuốn vào đó hàng nghìn người là một giải pháp logic hơn, đương nhiên phải đảm bảo rằng chương trình mang lại những kết quả có thể chấp nhận được trong việc phát hiện hành vi bất hợp pháp. Ngoài ra, dù rằng nhiều người với các trình độ chuyên môn kỹ thuật cao có thể đóng vai trò giám sát như thế, nhưng theo một viễn cảnh khác thì để làm như vậy nó có thể là điều không đáng thèm muốn. Ngay cả các chuyên gia tinh tuý nhất cũng có thể bỏ sót các kiểu hành vi bất hợp pháp nào đó có trong số lượng hành động khổng lồ diễn ra trong các hệ thống và các mạng hiện nay. Do vậy, một chương trình phát hiện xâm nhập phù hợp có thể không quét hết hành động mà các chuyên gia bỏ sót.

Thực ra phát hiện không phải là mục đích duy nhất của phát hiện xâm nhập. Một lý do rất quan trọng khác để sử dụng IDSs là chúng luôn đáp ứng khả năng lập báo cáo. Một lần nữa, theo tưởng tượng thì ở trường hợp tồi nhất thường vẫn dựa vào một số lượng người đáng kể tiến hành thu thập dữ liệu thâm nhập, khi đó mỗi người dùng một định dạng khác nhau để ghi chép dữ liệu, cộng thêm việc sử dụng những thuật ngữ và đặc tả khó hiểu đối với mọi người trừ người đó. Việc cố gắng tập hợp dữ liệu và các mô tả của mỗi người giám sát để thu được các mẫu và phương hướng hầu như không thể thực hiện được; việc tạo ra khả năng phán đoán

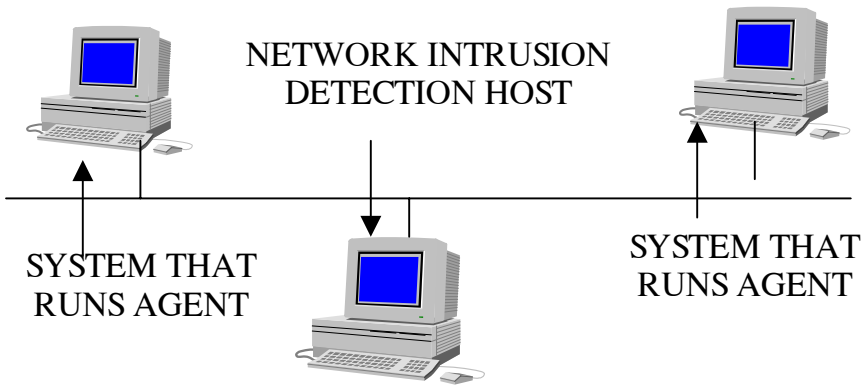
không dựa vào bất cứ dữ liệu nào của người giám sát luôn là một thách thức thực sự. Một hệ thống phát hiện xâm nhập hiệu quả đảm bảo khả năng lập báo cáo không chỉ đem lại những bản trình bày thông tin thân thiện với con người mà còn là những giao diện với một CSDL trung tâm cũng như khả năng khác cho phép lưu trữ, phục hồi và phân tích dữ liệu hiệu quả.

### 1.3- IDSs làm việc như thế nào?

IDSs làm việc theo các cách thức rất khác nhau liên quan tới kiểu dữ liệu mà chúng thu được cũng như các kiểu phân tích mà chúng thực hiện. Ở mức sơ đẳng nhất, một chương trình chạy trên một hoặc nhiều máy nhận bản ghi dữ liệu kiểm tra từ máy đó. Chương trình tìm kiếm những dấu hiệu của hành vi bất hợp pháp thông qua mỗi đầu vào trong các bản ghi kiểm tra. Loại chương trình này là một bộ phận của IDS dựa vào máy chủ hay hệ thống. Ở mức đặc biệt khác, một IDS có thể được phân loại theo bản chất (MUKH94). Phần mềm (thường nói đến như một phần mềm  trung gian) thuộc về một hay nhiều hệ thống được kết nối thành một mạng. Phần mềm quản lý trong một server cụ thể nhận dữ liệu từ các agent nó nhận biết được và phân tích dữ liệu (CROS95). Giải pháp thứ hai này đặc trưng cho một IDS dựa vào mạng (xem hình 1).

Lưu ý rằng nếu dữ liệu mà mỗi agent gửi tới nơi quản lý không bị làm xáo trộn, thì mức độ phân tích có thể có hiệu quả hơn so với các IDS dựa vào máy chủ hay hệ thống vì một vài lý do sau:

1. Mặc dầu IDS dựa vào máy chủ có thể không phụ thuộc vào dữ liệu kiểm soát (nếu nó có dịch vụ thu thập dữ liệu riêng của nó độc lập với kiểm soát), dữ liệu kiểm soát và các kiểu dữ liệu sản sinh trong các hệ thống đơn lẻ là đối tượng để giả mạo và/hoặc xoá. Một kẻ tấn công làm mất hiệu lực kiểm soát và/hoặc dịch vụ thu thập dữ liệu xâm nhập trên một máy định trước sẽ thực sự vô hiệu hoá IDS chạy trên máy đó. Tuy nhiên, điều này không đúng trong trường hợp IDS dựa vào mạng, cái mà có thể thu thập dữ liệu từ các máy riêng lẻ, các thiết bị thụ động (ví dụ những bộ phân tích giao thức) và các máy khó đánh bại hơn, chẳng hạn những filewall. Nói cách khác, các IDS dựa vào mạng không phụ thuộc vào dữ liệu từ các hệ thống riêng lẻ.



*Hình 1*. Triển khai của một IDS mà trong đó chạy phần mềm trung gian trên các máy chủ, IDS gửi dữ liệu tới bộ phát hiện xâm nhập mạng trung tâm để phân tích.

2. Hơn nữa, các IDS dựa vào mạng có thể dùng dữ liệu mà không phải sẵn có trong các IDS dựa vào hệ thống (HERR97). Ví dụ, xem xét một kẻ tấn công đăng nhập vào một hệ thống với tên người dùng "BROWN", sau đó đăng nhập vào một hệ thống khác trên cùng mạng với tên "SMITH". Phần mềm quản lý có thể gán một ID mạng cho mỗi người dùng, vì thế cho phép nó nhận biết có một người dùng có bản đăng nhập trong cả hai hệ thống. Sau đó, căn cứ vào thực tế IDS này có thể đưa ra báo động rằng người dùng trong ví dụ này đã đăng nhập vào các tài khoản khác nhau với những tên khác nhau. Không thể có mức độ phân tích này nếu một IDS không có dữ liệu từ nhiều máy trên mạng.

Một dạng hệ thống ID thứ ba hiện nay khá phổ biến liên quan tới một hoặc nhiều hệ thống theo dõi lưu thông của mạng (thường tại vị trí biên chẳng hạn gần filewall) và xem xét lưu thông gói có dấu hiệu xấu. Các "hệ thống phát hiện xâm nhập mạng" này dễ triển khai khi cần bảo vệ một cơ quan khỏi cuộc tấn công từ bên ngoài, nhưng chúng có mặt hạn chế là thiếu cách xử lý bên trong mà cũng có thể cần quan tâm.

## **2-** CÁC GIẢI PHÁP PHÁT HIỆN XÂM NHẬP

Các cài đặt IDSs khác nhau làm việc không chỉ sử dụng các loại dữ liệu và phương pháp phân tích khác nhau về cơ bản, mà chúng còn khác nhau về các kiểu giải pháp phát hiện xâm nhập đã được đưa vào thiết kế của chúng. Câu hỏi đúng đắn ở đây không phải là "Bạn muốn triển khai hệ thống phát hiện xâm nhập (IDS) hay không?" mà là "Bạn muốn triển khai kiểu IDS nào?". Có các kiểu IDS chính như sau:

### **2.1- Các hệ thống phát hiện dị thường**

Các hệ thống phát hiện dị thường được thiết kế để khám phá cách xử lý dị thường, nghĩa là cách xử lý không theo ý muốn và khác thường. Ở mức sơ đẳng nhất, các hệ thống phát hiện dị thường xem xét việc sử dụng một hệ thống máy tính trong suốt thời gian một ngày hoặc đêm ở nơi mà người dùng hợp pháp từng khó sử dụng máy tính. Các bản sơ lược thống kê chỉ ra những phần trăm xử lý có thể thành công và cái gì nằm trong giải cho phép độ lệch chuẩn về một chỉ tiêu nào đó, và vì vậy lộ ra cơ sở để xác định có hành động nào của người dùng là không dị thường. Ở mức phức tạp hơn, có thể mô tả sơ lược các biến thiên và các quy trình, chẳng hạn các kiểu sử dụng quen thuộc của mỗi người dùng cụ thể. Ví dụ, một người dùng có thể truy nhập server hầu như để đọc thư; một người khác có thể cân bằng thời gian sử dụng giữa thư và các ứng dụng dựa vào bảng tính; và người thứ ba có thể hầu như viết và dịch các chương trình. Nếu người thứ nhất bỗng nhiên bắt

đầu dịch chương trình, thì hệ thống phát hiện dị thường nên báo hiệu kiểu hành vi này khi nghi ngờ.

### 2.2- Các hệ thống phát hiện lạm dụng

Tiêu điểm chính của các hệ thống phát hiện lạm dụng là chống lại nguy cơ lạm dụng của những người dùng được cấp phép. Những nguy cơ này bao gồm các cuộc đăng nhập không được phép hay những cố gắng đăng nhập xấu tới các hệ thống nhằm lạm dụng các dịch vụ (ví dụ, các dịch vụ dựa vào Web, thiết lập file hệ thống,...) mà những người dùng không cần xác nhận bản thân họ. Vì thế, trong trường hợp sau các hệ thống phát hiện lạm dụng tốt sẽ định danh những mẫu (gọi là những "dấu hiệu") hành động dị thường cụ thể. Ví dụ, nếu một người dùng FTP không bình thường đưa vào nhiều lần dòng lệnh cd.., thì đó là một cơ hội tốt để người dùng đang cố gắng tấn công "dotdot" đi đến thư mục mức cao hơn truy nhập FTP cho phép như giả định. Nó rất khác với việc một người dùng hợp pháp thường vẫn bấm những phím này nhiều lần.

### 2.3- Các hệ thống giám sát đích

Các hệ thống giám sát đích có một sự sai lệch căn bản đôi chút với các hệ thống đề cập trước đó vì chúng không cố gắng phát hiện những cái không bình thường hay sự lạm dụng. Thay vào đó, chúng báo cáo các đối tượng đích nào đó đã bị thay đổi chưa, nếu có thì một tấn công có thể đã xảy ra. Ví dụ, trong các hệ thống UNIX những kẻ tấn công thường thay đổi chương trình /sbin/login (nguyên nhân gây ra đăng nhập mạng giả tạo, khi đó mật khẩu của người dùng đang thử vào mạng bị thu giữ và lưu vào một file ẩn) hay file /etc/passwd (file chứa tên của những người dùng, mức đặc quyền và ...). Trong các hệ thống Windows NT, người nào đó có thể thay đổi các file .DLL (thư viện liên kết động) nhằm biến đổi cách xử lý của hệ thống. Hầu hết các hệ thống giám sát đích sử dụng một thuật toán mật mã để tính toán kiểm tra mật mã đối với mỗi file đích. Vì thế, nếu bản kiểm tra mật mã được tính ở lần sau và bản kiểm tra mật mã mới khác với bản trước đó thì IDS sẽ báo cáo về sự thay đổi đó. Mặc dầu kiểu IDS này bề ngoài dường như không phức tạp bằng các kiểu trước đây, nhưng nó có một vài ưu điểm hơn các các hệ thống phát hiện dị thường và lạm dụng:

1. Khi những kẻ xâm nhập can thiệp vào các hệ thống, chúng thường xuyên tạo ra sự thay đổi (đôi khi là tình cờ, đôi khi là cố ý). Cho nên, những file, những cái có thể thi hành được bị thay thế bởi một Trojan Horse và do đó lộ ra những dấu hiệu rõ nét về một cuộc tấn công đã xảy ra.

2. Các hệ thống giám sát đích không dựa vào các tiêu chuẩn thống kê, những dấu hiệu và các công cụ chỉ báo khác mà rất có thể không chắc chắn. Vì thế, các hệ thống này không như là mô hình phụ thuộc. Chúng đơn giản và không phức tạp. Hơn nữa, chúng thực sự không cần phê chuẩn vì tính logic sau chúng là khá hiển nhiên.

3. Chúng không phải chạy liên tục để có hiệu quả. Tất cả chúng phải làm là chạy một chương trình giám sát đích tại một điểm đúng giờ, sau đó là cái khác. Vì thế, các hệ thống giám sát đích nói chung không đưa đến tổng chi phí thực hiện nhiều như các kiểu IDS khác.

### 2.4- Các hệ thống thực hiện tương quan diện rộng của những thăm dò kéo dài và "lén lút"

Không phải mọi tấn công xảy ra đều là tấn công tổng lực. Một mẫu tấn công khá điển hình là kiểu tấn công mà trước hết những kẻ xâm nhập thăm dò các thành phần hệ thống và mạng từ xa chẳng hạn các router ở những chỗ yếu liên quan tới an toàn, sau đó mới thực sự lao vào tấn công. Nếu cùng một lúc những kẻ tấn công tiến hành một số lượng lớn thăm dò, thì rất có khả năng gây sự chú ý đặc biệt. Vì thế, những kẻ tấn công thăm dò một hệ thống nhiều lần, sau đó là một cái khác, rồi đến cái khác nữa trong những khoảng thời gian kéo dài một cách thận trọng. Kết quả là làm giảm đáng kể khả năng chú ý đến những thăm dò. Kiểu IDS thứ tư đưa ra mối tương quan diện rộng của những thăm dò kéo dài và lén lút nhằm phát hiện kiểu tấn công.

## 3-NHỮNG ƯU ĐIỂM VÀ HẠN CHẾ CHÍNH CỦA CÔNG NGHỆ PHÁT HIỆN XÂM NHẬP

### 3.1-Ưu điểm

Về tiềm lực thì phát hiện xâm nhập là khả năng mạnh nhất mà thủ tục an toàn thông tin có thể triển khai. Nhiều khả năng phạm tội và lạm dụng máy tính của những kẻ tấn công phụ thuộc vào khả năng của họ để trốn tránh sự chú ý cho đến khi nó là quá muộn. Những thống kê có liên quan của DISA được trích dẫn trên đây quả là đáng sợ; theo những phát hiện này, việc đặt ra câu hỏi "thực tế an toàn thông tin đòi hỏi phải theo dõi thường xuyên đến mức nào để có thể tránh sử dụng rộng rãi IDS" có lẽ là hợp lý hơn. Chúng ta nhấn mạnh rằng thực tế an toàn thông tin nào đó không dùng công nghệ IDS sẽ không được rèn luyện thường xuyên vì đương nhiên nó sẽ không nhận thấy phần lớn những sự cố xảy ra. Bất cứ thực tế nào không có ý thức về những sự cố sẽ không hiểu được nhân tố rủi ro thực sự; đáng buồn là người ta chỉ bắt chước cách xử sự của con đà điểu với cái đầu trong cát (tự mình dối mình). Diễn đạt một cách đơn giản, một IDS hiệu quả có thể cải thiện rất lớn khả năng phát hiện và thông báo những sự cố liên quan tới an toàn.

Chúng ta cũng phải lưu ý độ phức tạp về cấu hình của đa số các hệ thống và chất lượng nghèo nàn của hầu hết phần mềm thương mại cũng đủ đảm bảo những thiếu sót mới sẽ bị phát hiện và thông báo rộng rãi có thể được sử dụng chống lại hầu hết các môi trường tính toán. Những giải quyết tạm thời và các rào chắn không sẵn có như các công cụ tấn công, và các rào chắn dựa vào việc giám sát và đối phó chỉ là cách giảm nhẹ những mối nguy hiểm  rất lớn. Sự thất bại vì sử dụng các cơ chế như thế chính là do không cung cấp đủ các kiểm soát an toàn thông minh.

Để tăng cường khả năng dự báo và đối phó với các sự cố, các hệ thống phát hiện xâm nhập có một vài lợi ích chính khác, bao gồm:

1. Giảm giá thành. Những khả năng tự động hoá về thời gian nhìn chung có giá thành thấp hơn con người khi thực hiện cùng chức năng. Một khi tổ chức đã trả tiền để mua và cài đặt một hoặc nhiều IDS, giá của khả năng phát hiện xâm nhập là hoàn toàn hợp lý.

2. Tăng khả năng phát hiện. Như đã đề cập trước đây, một IDS hiệu quả có thể thực hiện nhiều phân tích phức tạp (ví dụ, bằng việc thu thập dữ liệu từ phạm vi nguồn rộng lớn) hơn con người. Con người kiểm tra vấn đề đọc và dịch dữ liệu thông qua các bản ghi kiểm tra (audit log) của các hệ thống. Các bản ghi này đặc biệt sản sinh một khối lượng lớn dữ liệu mà những người quản trị hệ thống hiếm có thời gian để kiểm tra, ít nhất ở một chi tiết nào đó. Cũng nên nhớ lại rằng những kẻ tấn công thường đặt mục tiêu ban đầu là phá hỏng bản ghi kiểm tra một khi họ làm tổn thương các rào chắn của hệ thống. IDSs không cần dựa vào các bản ghi nhật ký.

3. Giá trị ngăn chặn. Những kẻ tấn công khi nhận thấy khả năng phát hiện xâm nhập sẽ không sẵn lòng tiếp tục hành động bất hợp pháp liên quan tới máy tính. Vì thế, ở chừng mực nào đó IDSs đáp ứng việc ngăn chặn hành vi bất hợp pháp.

4. Thông báo. Một IDS hiệu quả gắn liền với khả năng thông báo sử dụng những định dạng chuẩn, dễ đọc hiểu và những khả năng quản lý dựa vào dữ liệu.

5. Pháp lý. Một vài IDS gắn liền với những khả năng pháp lý. Chúng liên quan tới việc đưa ra chứng cớ thích đáng có thể được sử dụng ở toà án. Mục tiêu chính của những khả năng pháp lý là thu thập và bảo quản chứng cớ về tội phạm và sự lạm dụng máy tính sẽ được thừa nhận tại toà án.

6. Phát hiện hỏng hóc và khôi phục. Nhiều hỏng hóc bộc lộ những nét đặc trưng tương tự với lạm dụng hay xâm nhập. Việc triển khai IDSs tốt có thể dẫn đến thúc đẩy sự chú ý tới những triệu chứng này trước khi chúng bị hỏng hoàn toàn. Hơn nữa, một số IDS có thể cung cấp dữ liệu kiểm tra về những thay đổi cho phép phục hồi hoặc kiểm tra lại các thành phần hỏng hóc một cách nhanh chóng hơn.

### 3.2-Những nhược điểm

Phát hiện xâm nhập cũng mang theo nhiều hạn chế. Một số đáng chỉ trích nhất trong các hạn chế này bao gồm:

1. Sự non nớt. Hầu hết (không phải tất cả) IDS hiện nay đều có những hạn chế đáng kể về chất lượng chức năng tiện ích mà chúng cung cấp. Một số chỉ hơn chút ít so với các mẫu đầu tiên cùng với giao diện người dùng phức tạp. Những cái khác có mục đích là so sánh các dấu hiệu từ một thư viện dấu hiệu với các sự kiện xảy ra trong các hệ thống và/hoặc các mạng, nhưng các nhà sản xuất hay những người phát triển từ chối cho phép những khách hàng tương lai học cách làm thế nào hoàn chỉnh và làm cho các thư viện này phù hợp. Mối lo lắng tương tự là thực tế các kiểu tấn công mới xảy ra bất cứ lúc nào; nếu không có một ai đó cập nhật thư viện dấu hiệu thì hiệu quả phát hiện sẽ giảm đi. Vẫn còn IDSs khác dựa vào các chỉ báo thống kê chẳng hạn "các mẫu sử dụng thông thường" đối với mỗi người dùng. Tuy nhiên, thủ phạm thông minh có thể kiên nhẫn và liên tục làm hành động không rơi ra ngoài phạm vi thông thường mà trở thành che giấu việc làm đó. Do đó thủ phạm có thể điều chỉnh tiêu chuẩn thống kê về thời gian. Ai đó thường sử dụng hệ thống trong khoảng từ 8 giờ sáng đến 8 giờ chiều có thể muốn tấn công hệ thống vào lúc nửa đêm. Giả dụ thủ phạm chỉ tấn công hệ thống vào nửa đêm, các bộ phận báo động có lẽ không làm việc vì IDS có thể không cho là việc sử dụng lúc nửa đêm nằm trong phạm vi thông thường của người dùng đó. Nhưng nếu thủ phạm tiếp tục sử dụng hệ thống từ 11 giờ sáng đến 11 giờ đêm hàng ngày trong một tuần, thì việc sử dụng vào nửa đêm có lẽ không được cho là làm chệch hướng thống kế nữa.

2. Những phát hiện sai. Một hạn chế nghiêm trọng khác của IDSs hiện nay là những phát hiện sai (sai lầm loại 1). Một phát hiện sai xảy ra khi IDS báo hiệu một sự kiện dẫn đến vi phạm an toàn, nhưng sự kiện đó thực sự không liên quan đến sự vi phạm đó. Nhiều lần vào mạng hỏng do người dùng quên mật khẩu của họ là một ví dụ. Hiện nay hầu hết các khách hàng IDS đều quan tâm tới những báo động sai vì chúng thường phá vỡ và đánh lạc hướng những người điều tra nghiên cứu những cuộc xâm nhập giả rời xa những công việc khác thật sự quan trọng.

3. Suy giảm hiệu suất. Việc triển khai IDSs đã đánh vào hiệu suất của hệ thống và/hoặc mạng. Lượng suy giảm thực tế phụ thuộc vào IDS cụ thể; một số thực sự phá vỡ hiệu suất. Các hệ thống dựa vào dị thường thường hay suy giảm nhất vì độ phức tạp của sự tương xứng cần thiết.

4. Chi phí ban đầu. Chi phí triển khai IDSs ban đầu có thể rất cao. Khi các nhà sản xuất bán sản phẩm của họ, họ thường chỉ đề cập tới giá mua. Chi phí triển khai các hệ thống này có thể đòi hỏi nhiều giờ tư vấn, kết quả là giá thành cao hơn nhiều so với dự tính ban đầu.

5. Khả năng dễ bị tấn công. Bản thân IDSs có thể bị tấn công làm mất những khả năng thực hiện của chúng. Trường hợp hiển nhiên nhất là khi nhân viên được uỷ thác trông nom tắt mọi IDS, tiến hành một loạt các

hành động bất hợp pháp, sau đó chạy lại tất cả IDSs. Bất kỳ một kẻ tấn công nào cũng có thể làm ngập hệ thống được sử dụng bởi các khả năng IDS với những sự kiện vô dụng làm phóng đại khoảng trống đĩa dùng cho dữ liệu IDS, do đó dẫn tới dữ liệu hợp pháp bị ghi đè lên, các hệ thống bị đổ vỡ và kéo theo một loạt tác động khác.

6. Tính khả dụng. IDSs được thiết kế để khám phá các cuộc xâm nhập không được phép truy nhập vào hệ thống. Tuy vậy, trong năm qua (vào thời gian bài này được viết) một tỷ lệ lớn các cuộc tấn công được báo cáo là những điều tra thăm dò (ví dụ, sử dụng các chương trình quét để khám phá những chỗ yếu trong các hệ thống) hoặc những tấn công từ chối dịch vụ. Giả sử một kẻ tấn công muốn làm đổ vỡ nhiều hệ thống trong mạng của một tổ chức ở mức có thể. Tại đó IDSs bất kỳ có thể không có khả năng phát hiện và thông báo nhiều tấn công từ chối dịch vụ ở vị trí đầu tiên. Ngay cả nếu chúng có khả năng làm như vậy, thì việc nhận ra rằng "Đúng, có một cuộc tấn công từ chối dịch vụ" cũng khó giúp gì nếu các hệ thống bị tấn công đã bị đánh gục! Thêm nữa, nhiều (nếu không phải hầu hết) IDSs hiện nay làm công việc phát hiện những cuộc tấn công khởi nguồn từ bên ngoài tốt hơn nhiều so với việc phát hiện những cuộc tấn công bắt nguồn từ nội bộ. Không may, đã chỉ ra rằng triển vọng mất mát từ các cuộc tấn công nội bộ cao hơn nhiều so với các cuộc tấn công từ bên ngoài.

7. Dễ bị giả mạo. IDSs có khả năng dễ bị giả mạo bởi những cá nhân không được cấp phép cũng như được cấp phép. Có nhiều cách đánh bại IDSs được biết rộng rãi trong cả các nhóm an toàn thông tin và các nhóm thủ phạm. Trong một bài báo rất hấp dẫn, Cohen mô tả 50 trong số các cách này (COHE97).

8. Thay đổi công nghệ. Việc phụ thuộc vào công nghệ cụ thể có thể dẫn đến mất tính bảo vệ khi toàn bộ cơ sở hạ tầng tính toán thay đổi. Ví dụ, phát hiện xâm nhập dựa vào mạng thường bị chặn lại bởi các mạng IP dựa vào chuyển mạch, các mạng tựa ATM, VPNs, mã hoá .... Tất cả các công nghệ này đang được triển khai rộng rãi hơn vào thời gian tới.

Các ưu điểm và nhược điểm của kỹ thuật phát hiện xâm nhập được tóm tắt ở bảng sau

| ƯU ĐIỂM | NHƯỢC ĐIỂM |
|---|---|
| Giảm chi phí (ít nhất về thời gian) do tính tự động. | Nhiều IDSs không cung cấp chức năng cần thiết |
| Hiệu quả phát hiện sự cố tăng. | Mức độ báo động sai cao không thể chấp nhận. |
| Có thể ngăn chặn hành vi bất hợp pháp. | Nói chung làm suy giảm hiệu suất |
| Xây dựng báo cáo, quản lý dữ liệu và các chức năng khác. | Chi phí ban đầu có thể quá cao |
| Thiết lập những khả năng pháp lý | Có thể sinh ra dữ liệu vô dụng |
| | Bản thân IDSs dễ bị tấn công |

## 4-ƯỚC ĐỊNH CÁC YÊU CẦU PHÁT HIỆN XÂM NHẬP

### 4.1-Mối quan hệ của pháp hiện xâm nhập với rủi ro

Một số lớn các tổ chức bắt đầu tiến trình quản lý rủi ro bằng việc thực hiện định kỳ những đánh giá về rủi ro, xác định số lượng các tài nguyên sẵn có, sau đó phân phối các tài nguyên theo một số phương pháp trong chiến lược giảm nhẹ rủi ro dựa vào độ ưu tiên, ví dụ cài đặt một hay nhiều kiểm soát chống lại rủi ro với khả năng tác động tiêu cực lớn nhất, sau đó đưa vào một hoặc nhiều biện pháp nhắm vào rủi ro có ảnh hưởng tiêu cực lớn thứ hai, và tiếp tục cho đến khi tài nguyên được dùng hết. Bất chấp việc có tương thích với mô hình hoạt động này hay không, nó đảm bảo rằng phát hiện xâm nhập sẽ được xem xét. Theo ngôn ngữ đơn giản, phát hiện xâm nhập không nhắm trực tiếp vào bất cứ rủi ro cụ thể nào như các biện pháp chẳng hạn các giải pháp mã hoá và xác thực của người thứ ba.

### 4.2-Khai thác các yêu cầu liên quan tới kinh doanh

Bất cứ công việc gì, trừ việc xử lý dễ dàng, đều là việc phát triển các yêu cầu cụ thể liên quan tới công việc có quan tâm đến phát hiện xâm nhập. Trong tất cả khả năng có thể xảy ra, khó khăn của việc làm này là một trong những người gièm pha trong tổ chức chiến đấu với khả năng phát hiện xâm nhập. Hơn nữa, các đơn vị kinh doanh có thể vô cùng miễn cưỡng khi dùng kỹ thuật phát hiện xâm nhập vì mức yêu cầu đặc trưng về tài nguyên (nhân viên và tiền bạc) và vì kỹ thuật này có thể bề ngoài dường như không liên quan tới các nhu cầu của các đơn vị kinh doanh có nhịp độ phát triển nhanh trong những môi trường thương mại ngày nay.

Mặt khác, việc mời được các đơn vị kinh doanh mua và phát triển các yêu cầu kinh doanh đối với phát hiện xâm nhập ở cấp độ đơn vị kinh doanh dù sao chăng nữa không phải là mục tiêu chính. Trong hầu hết các tổ chức, nếu kỹ thuật phát hiện xâm nhập chịu thử thách thành công, thì nó phải được được đưa vào như một khả năng trọng tâm. Các yêu cầu kinh doanh và cơ sở kinh doanh hợp lý đối với kỹ thuật phát hiện xâm nhập gần như có quan hệ chặt chẽ với các yêu cầu đối với chức năng kiểm soát của tổ chức. Mục tiêu tối thiểu của kỹ thuật phát hiện xâm

nhập trong các phạm vi kinh doanh là nhu cầu đánh giá một cách độc lập tác động của các mô hình sử dụng hệ thống và mạng dưới dạng những mối quan tâm về tài chính của tổ chức. Hiểu theo nghĩa hẹp thì dễ dàng nhất là đặt kỹ thuật phát hiện xâm nhập ở nơi nắm giữ chức năng kiểm tra của tổ chức.

**4.3-Tiêu chuẩn quyết định**

Giả sử rằng tổ chức của bạn quyết định đưa vào kỹ thuật phát hiện xâm nhập. Sau khi bạn tìm thấy nguồn gốc các yêu cầu kinh doanh gắn với tổ chức của bạn, thì bước thích hợp tiếp theo là xác định tổ chức của bạn sẽ đặt xây dựng IDS hay mua phiên bản thương mại, không sát thực tế. Nhìn chung chiến lược sau khôn ngoan hơn nhiều - việc xây dựng một IDS tuỳ chọn nói chung đòi hỏi thời gian và tài nguyên nhiều hơn nhiều so với bạn có thể hình dung từ trước đến giờ. Thêm nữa, việc duy trì các IDS theo đặt hàng nói chung là một sai lầm về mặt các hoạt động và chi phí lâu dài. Trường hợp ngoại lện là triển khai một công nghệ phát hiện xâm nhập hết sức đơn giản. Ví dụ, cài đặt và triển khai các "honey pot" server là một chiến lược như thế. Các honey pot server là các server báo động kết nối với mạng cục bộ. Thông thường không ai sử dụng honey pot server, nhưng máy chủ này được gán một cái tên làm chú ý nhưng không có thật (giả) (ví dụ, patents.corp.com). Nếu bất kỳ ai vào mạng hoặc ngay cả thử vào mạng, thì phần mềm trong server loại này báo cho người quản trị mạng, có lẽ bằng cách nhắn tin cho người quản trị. Chức năng chính của honey pot server là chỉ báo có hay không một người dùng bất hợp pháp "hành động bừa bãi trên mạng" để một hay nhiều cá nhân có thể bắt đầu biện pháp đối phó sự cố phù hợp. Chiến lược này không tinh tế về khả năng phát hiện xâm nhập mà nó cung cấp, nhưng nó đơn giản và hiệu quả rất đáng kể. Tốt hơn cho đến bây giờ, một nền hệ thống cũ, thấp vừa phải (ví dụ, Sparcstation 5) nói chung là quá đủ cho kiểu triển khai này.

Việc mua một sản phẩm IDS thương mại dễ dàng hơn khi cần đánh giá một cách có hệ thống chức năng tiện ích và các đặc trưng của mỗi sản phẩm được đề cử dựa vào tiêu chuẩn có ý nghĩa. Chúng tôi đề xuất ở mức tối thiểu tiêu chuẩn sau để bạn áp dụng:

1. Chi phí. Điều này bao gồm cả các chi phí trước mắt và lâu dài. Như đã đề cập trước đây, một số có thể xuất hiện chi phí nhỏ bé vì giá mua chúng thấp, nhưng những chi phí triển khai có thể không chịu đựng nổi.

2. Chức năng. Ở đây sự khác nhau giữa một IDS dựa vào hệ thống với IDS dựa vào mạng là rất quan trọng. Nhiều hệ chuyên gia phát hiện xâm nhập khẳng định rằng IDSs dựa vào hệ thống phát hiện hành động trong nội bộ tốt hơn, ngược lại IDSs dựa vào mạng phát hiện những cuộc tấn công từ bên ngoài tốt hơn. Tuy nhiên, mối quan tâm này chỉ là điểm bắt đầu với khía cạnh xác định có một chức năng tiện ích của sản phẩm phù hợp hay không. Sự hiện diện hay vắng mặt của các chức năng, chẳng hạn thông

báo các khả năng, tính đúng đắn của dữ liệu từ nhiều hệ thống và báo động sát với thời gian thực cũng quan trọng để xem xét.

3. Khả năng mở rộng. Mỗi công cụ đề cử nên cân đối không chỉ với các yêu cầu kinh doanh mà còn với các môi trường triển khai nó. Nói chung, tốt nhất nên giả thiết rằng bất cứ sản phẩm nào được mua sẽ phải tương xứng với sự vận động đi lên theo thời gian, như vậy việc có được một sản phẩm có thể đáp ứng không chỉ với môi trường hiện tại, mà còn với các môi trường phức tạp hơn luôn là một ý tưởng tốt.

4. Mức độ tự động. Nhiều tính năng của một sản phẩm IDS là tự động, càng ít sự can thiệp của con người càng tốt.

5. Độ chính xác. Một sản phẩm IDS không chỉ nhận biết sự xâm nhập có chủ ý nào đó xảy ra, mà cũng nên giảm thiểu mức độ báo động sai.

6. Khả năng tương tác. IDSs hiệu quả có thể tương tác với mỗi IDS khác để tạo nên dữ liệu khả dụng rộng rãi đối với các máy chủ khác thực hiện quản lý phát hiện xâm nhập và quản lý CSDL.

7. Dễ thao tác. Người ta muốn có một IDS dễ triển khai và bảo trì hơn là một cái không có khả năng đó.

8. Ảnh hưởng tới những hoạt động đang diễn ra. Một IDS hiệu quả ít gây ra đổ vỡ trong các môi trường mà nó tồn tại.

## **5-** KHAI THÁC KIẾN TRÚC PHÁT HIỆN XÂM NHẬP

Sau khi các yêu cầu đã có và kiểu IDS được sử dụng đã được chọn, giai đoạn hợp lý tiếp theo là khai thác kiến trúc để phát hiện xâm nhập. Trong ngữ cảnh hiện tại, thuật ngữ "kiến trúc" được định nghĩa như một mô tả đặc điểm mức cao về các thành phần khác nhau trong thực hành an toàn được tổ chức như thế nào và chúng quan hệ như thế nào với mỗi mục tiêu thực tế. Ví dụ, xem xét các thành phần của một thực tiễn an toàn thông tin trình bày ở hình 2.


*Hình 2*. Cơ cấu tổ chức đơn giản một kiến trúc an toàn

Để khai thác một kiến trúc phát hiện xâm nhập, nên bắt đầu ở mức cao nhất, đảm bảo rằng các chính sách bao gồm những sự chuẩn bị thích đáng cho việc triển khai, quản lý và tiếp cận kỹ thuật phát hiện xâm nhập. Ví dụ, một phát biểu chính sách nào đó đảm bảo không có người làm công hay người thầu khoán nào sẽ truy nhập hay thay đổi bất kỳ IDS nào được triển khai. Một phát biểu chính sách khác sẽ định rõ có bao nhiêu dữ liệu phát hiện xâm nhập được thu giữ và chúng phải được lưu trữ như thế nào. Nó cũng quan trọng để đảm bảo rằng một chính sách an toàn thông tin của tổ chức tuyên bố rõ ràng cái gì cấu thành "hành vi bất hợp pháp" nếu đầu ra của IDSs có một ý nghĩa thực sự nào đó.

Ở mức tiếp theo bên dưới, ai đó có thể thảo ra các chuẩn cụ thể tương ứng với mỗi kiểu IDS được triển khai. Ví dụ, đối với IDSs cùng thư viện dấu hiệu thì quan trọng là định rõ các thư việc sẽ được nâng cấp thường xuyên như thế nào. Ở mức thấp nhất có thể có những khuyến cáo, chẳng hạn bao nhiêu khoảng trống đĩa dùng cho mỗi cài đặt IDS cụ thể. Điều này là quan trọng giúp nhận thức rõ một khả năng phát hiện xâm nhập không làm việc tốt khi bị cô lập; nó cần phải là một bộ phận của kết cấu bên trong của việc mở mang tổ chức. Chính vì vậy, việc khai thác một kiến trúc phát hiện xâm nhập là một bước rất quan trọng trong quá trình triển khai thành công kỹ thuật phát hiện xâm nhập. Cũng lưu ý rằng việc triển khai một kiến trúc như thế không đơn giản như các biểu đồ có thể bao hàm trong hình 2; nó yêu cầu phân tích một cách cẩn thận các yêu cầu phát hiện xâm nhập đối với mỗi thành phần của kiến trúc chính xác là cái gì, và làm thế nào để bao gồm cả giải pháp cho mỗi nhu cầu trong thành phần đó. Quan trọng không kém, nó đòi hỏi sự đồng tâm trong các tổ chức sẽ hoặc có thể chịu ảnh hưởng bởi sự giới thiệu về thiết bị kỹ thuật phát hiện xâm nhập mới nhập từ nhà quản lý có uy tín.

## **6-** KẾT LUẬN

Chúng ta đã khảo sát về phát hiện xâm nhập và vai trò tiềm năng của nó trong thực tiễn an toàn thông tin, chống lại lý lẽ "tâm lý pháo đài" dẫn tới việc cài đặt biện pháp kiểm soát an toàn chẳng hạn như kiểm tra mật khẩu mà không nhận ra rằng không có biện pháp phòng thủ nào có hiệu quả 100%. Vì thế, quan trọng là dành một phần thích đáng tài nguyên của tổ chức cho việc phát hiện những sự cố xảy ra và đối phó hiệu quả với chúng. Chúng ta đã đưa ra một cái nhìn về những ưu điểm và nhược điểm của nó, sau đó đã thảo luận xem làm thế nào để có thể đưa kỹ thuật phát hiện xâm nhập vào tổ chức một cách hiệu quả. Cuối cùng, chúng ta đã diễn giải những mối quan tâm liên quan tới việc triển khai IDSs.

Về nhiều mặt, phát hiện xâm nhập có cùng bước ngoặt mà kỹ thuật filewall đã có một thập kỷ trước. Các filewall trước đây thực sự khá nguyên sơ và hầu hết các tổ chức xem chúng như là mối quan tâm nhưng không thực tế. Kỹ thuật phát hiện xâm nhập đã sẵn có trước khi filewall đầu tiên được cài đặt, nhưng cái đi trước thường phải đối mặt với cuộc vật lộn khó khăn hơn. Vấn đề có thể được mô tả như thể thuộc về bí mật và sự lảng tránh đã bao quanh IDSs. Các filewall trực tiếp hơn

- filewalls đơn giản nhất thường là chặn đứng hoặc cho phép lưu thông đi đến máy chủ cụ thể. Khi mua một sản phẩm filewall, bạn có thể đủ lý do để chắc chắn rằng sản phẩm này sẽ làm việc như thế nào. Điều tương tự không đúng trong lĩnh vực phát hiện xâm nhập. Tuy vậy, cùng thời gian đó, phát hiện xâm nhập nhanh chóng giành được sự chấp thuận trong các tổ chức có uy tín trên toàn thế giới. Mặc dù, công nghệ xung quanh lĩnh vực này còn xa mới hoàn thiện, nhưng bấy giờ nó đủ tin cậy và tinh vi để cho phép triển khai.

Tin tức tốt lành cho hay mỗi năm kỹ thuật phát hiện xâm nhập càng trở nên tinh vi hơn. Cũng nhờ sự cổ vũ của thực tế là các vấn đề liên quan tới hiệu suất đi liền với IDSs đang trở nên tương đối ít quan trọng vì các hệ điều hành và nền phần cứng để chạy chúng không ngừng được cải tiến với sự lưu tâm tới các đặc trưng về hiệu suất. Thêm nữa, các nhóm nghiên cứu đang làm việc tốt hơn trong việc khám phá hướng đi cho thế hệ tiếp theo của kỹ thuật phát hiện xâm nhập. Một số tiến bộ hiện nay trong việc nghiên cứu phát hiện xâm nhập bao gồm các lĩnh vực như khả năng tương tác của IDSs, tự động thông báo và tự động đối phó (ở nơi mà IDS có hành động lảng tránh khi nó xác định được một cuộc tấn công đang diễn ra).

Cũng có tin xấu cho hay nếu tổ chức của bạn hiện tại không sử dụng kỹ thuật phát hiện xâm nhập, thì "tốc độ nội lực" phát hiện xâm nhập chậm tồi tệ. Hơn nữa, có ý kiến cho là một tổ chức mua, nhưng sau đó lại bị cuốn vào một sản phẩm IDS mới sẽ không có phương tiện sẵn sàng để hưởng những lợi ích tức thì. Một sự vòng vo học sử dụng kỹ thuật phát hiện xâm nhập rạch ròi, quá mức đang tồn tại. Nhưng dù là bây giờ bạn mới bắt đầu triển khai kỹ thuật này, thì thời gian tiêu tốn cũng xứng với tinh thần phát hiện xâm nhập và công nghệ kết hợp với nó trong giao lưu của tổ chức. Vì vậy, quan trọng là trở nên thân thiện với nó và bắt đầu sử dụng kỹ thuật này càng sớm càng tốt để tránh bị tụt hậu. Sự lựa chọn là tiếp tục hoạt động như câu thành ngữ đà điểu với cái đầu dưới cát.

## Tài liệu tham khảo


COHE97 Cohen, F., Managing network security- Part 14: 50 ways to defeat your intrusion detection system. *Network Security*, December, 1997, pp.11-14.

CROS95 Crosbie, M. and Spafford, E.H., Defending a computer system using autonomous agents. *Proceedings of 18th National Information System Security Conference*, 1995, pp. 549-558.

GARF96 Garfinkel, S. and Spafford, G., *Practical Unix and Internet Security,* O'Reilly & Associates, Inc., 1996.

GARF97 Garfinkel, S. and Spafford, G., *Web Security & Commerce*, O'Reilly & Associates, Inc., 1997.

HERR97 Herringshaw, C. Detecting attacks on networks. *IEEE Computer,* 1997, Vol, Vol. 30 (12), pp. 16-17.

MUKH94 Mukherjee, B., Heberlein, L. T., and Levitt, K.N., Network intrusion

detection. *IEEE Network*, 1994, Vol.8 (3), pp.26-41.

POWER99 Power Richard, Issues and Trends: 1999 CSI/FBI computer crime and security survey, *Computer Security Journal*, Vol.XV, No.2, Spring 1999.

SCHU96 Schultz, E.E. and Wack, J., Responding to computer security incidents, in M. Krause and H.F. Tipton (Eds.), *Handbook of Information Security*. Boston:Auerbach, 1996, pp.53-68.

VANW94 Van Wyk, K.R., Threats to DoD Computer Systems. Paper presented at 23rd Information Integrity Institute Forum

# CHƯƠNG 3
# THƯƠNG MẠI ĐIỆN TỬ

## 1. MỘT SỐ KHÁI NIỆM CƠ BẢN VỀ THƯƠNG MẠI ĐIỆN TỬ (TMĐT).

TMĐT là việc trao đổi thông tin thương mại thông qua các phương tiện điện tử. Các mối quan hệ trao đổi thông tin thương mại chủ yếu bao gồm: giao dịch cung cấp, trao đổi hàng hoá, thoả thuận phân phối, đại diện hoặc đại lý thương mại, uỷ thác hoả hồng, cho thuê, xây dựng công trình, tư vấn kỹ thuật, đầu tư, cấp vốn, ngân hàng, bảo hiểm, thoả thuận khai thác, liên doanh, chuyên chở hàng hoá,.... Theo ước tính của các chuyên gia trên thế giới cho đến nay TMĐT có trên 1300 lĩnh vực ứng dụng, trong đó buôn bán hàng hoá và dịch vụ chỉ là một trong số đó.

Các hình thức hoạt động chủ yếu của TMĐT là:

- Thư điện tử
- Thanh toán điện tử( trả tiền trực tiếp vào tài khoản, trả tiền mua hàng bằng thẻ mua hàng, thẻ tín dụng,...). Ngày nay thanh toán điện tử mở rộng sang các lĩnh vực là :
    - trao đổi dữ liệu điện tử tài chính giữa các đối tượng giao dịch với nhau bằng điện tử.
    - Tiền mặt Internet: là tiền được chuyển đổi tự do sang các loại tiền khác thông qua Internet bằng kỹ thuật số hoá.
    - Túi tiền điện tử, chủ yếu là thẻ thông minh, giữ tiền điện tử và chi trả khi chủ sử dụng xác thực là đúng.
    - Giao dịch thanh toán ngân hàng số hoá ( giữa các ngân hàng với nhau , với các đại lý thanh toán hoặc với khách hàng).
- Trao đổi dữ liệu điện tử: là sự trao đổi dữ liệu dưới dạng có cấu trúc từ máy tính điện tử (MTĐT) này sang MTĐT khác, giữa các công ty có thoả thuận với nhau một cách tự động. Công việc trao đổi dữ liệu điện tử chủ yếu bao gồm giao dịch kết nối, đặt hàng, gửi hàng, thanh toán.
- Truyền dung liệu. Dung liệu (content) là nội dung hàng hoá, mà không phải là bản thân vật mang nội dung đó, ví dụ như tin tức, nhạc, phim, các chương trình phát thanh, truyền hình, các chương trình phần mềm, các ý kiến tư vấn, nội dung các hợp đồng,...Hiện đã có khoảng 2700 tờ báo được đưa lên mạng Internet. Việc đặt mua chỗ trên máy bay, rạp hát qua Internet ở Mỹ chiếm tới 70% .
- Bán lẻ hàng hoá hữu hình. Người ta xây dựng các "cửa hàng ảo" (virtual shop) trên Internet. Việc xem hàng, xác nhận mua , trả tiền đều bằng giao dịch trên mạng. Tất nhiên là việc gửi hàng hữu hình vẫn theo cách truyền thống.

## 2. TÌNH HÌNH PHÁT TRIỂN TMĐT TRÊN THẾ GIỚI.

TMĐT đang phát triển rất nhanh trên toàn thế giới. Người ta chia quá trình phát triển của nó thành 3 giai đoạn:

1. ở giai đoạn thứ nhất các doanh nghiệp tham gia TMĐT bằng cách xây dựng các trang Web và kết nối với Internet để khách hàng có thể truy cập mọi thời gian trong ngày. Những trang Web này chủ yếu dùng để giới thiệu sản phẩm, quảng cáo hàng hoá dịch vụ.
2. ở giai đoạn thứ hai người ta đã tích hợp được hệ thống thông tin kinh doanh điện tử với máy chủ Web để cung cấp dịch vụ Internet. Trên các Website khách hàng đặt hàng, thông tin đặt hàng được tiếp nhận và chuyển tới hệ thống xử lý đơn đặt hàng và phân tích các thuộc tính đơn đặt hàng. Với hệ thống dữ liệu khách hàng chương trình sẽ tự động gửi E-mail chào hàng đến từng khách hàng.
3. Do trên mạng Internet chứa một khối lượng khổng lồ các trang Web của các loại hình kinh doanh nên xuất hiện nhu cầu đồng bộ hoá các thông tin kinh doanh điện tử và xử lý tự động các thông tin này, nên TMĐT giai đoạn thứ ba mà thế giới đang tiến đến hiện nay không định hướng vào trang Web mà định hướng vào khách hàng, người ta sẽ chuyển thông tin trực tiếp tới từng khách hàng; hệ thống sẽ tự động biết khách hàng cần thông tin gì, sẽ tự động biên dịch thông tin và gửi tới khách hàng. Trong giai đoạn này phần mềm sẽ cho phép các ứng dụng tự tương tác với nhau mà không cần sự can thiệp của con người. Một ứng dụng ở một đầu giao dịch có thể tự động truy nhập và trao đổi với nhiều nguồn thông tin cùng một lúc nhiều máy chủ của các doanh nghiệp trên mạng Internet và đồng bộ hoá các hệ thống thông tin này.

Có thể nói TMĐT ra đời và phát triển cùng với sự phát triển của Internet, tức là chủ yếu từ năm 1991. Việc phát triển của TMĐT phải đi song hành với sự phát triển của cơ sở hạ tầng về công nghệ và nhân lực (chủ yếu là công nghệ thông tin và nhân lực sử dụng công nghệ thông tin), bảo mật và an toàn, giao dịch tài chính tự động, hạ tầng kinh tế và pháp lý, bảo vệ sở hữu trí tuệ. Vì vậy thương mại điện tử phát triển trước tiên ở các nước phát triển.

Theo đánh giá của các chuyên gia Mỹ, năm 2002 thị trường TMĐT của thế giới sẽ đạt doanh thu khoảng 300 tỷ USD. Theo ban TMĐT Bộ Thương mại, doanh số đó có thể đã là 400 tỷ USD năm 2002 và 1300 tỷ USD năm 2003 (Intel Việt nam dự báo năm 2004 mới là 7292 tỷ USD). Mỹ hiện đang chiếm 70% trong tổng doanh số giao dịch bằng TMĐT của thế giới, đồng thời là nước cứ 100 gia đình có 38 gia đình có máy tính, đạt tỷ lệ cao nhất thế giới. Chi phí giao dịch của Mỹ cũng đạt cao nhất thế giới và chiếm khoảng 45% GDP.

Canada là nước phát triển cao về TMĐT với doanh số đạt 13 tỷ USD năm 2000.

Nhật bản cứ 100 gia đình có 20 gia đình có máy tính. Tổng giá trị giao dịch TMĐT giai đoạn 1999-2001 đạt 126,05 tỷ.

Liên minh Châu Âu (EU) đã ứng dụng TMĐT trong toàn bộ hệ thống ngân hàng, tuyền tin, truyền hình. Trong Liên minh Châu Âu Hà lan đứng vị trí hàng đầu với 38% gia đình có MTĐT và 33% số người giao dịch TMĐT qua Internet. Trung quốc có tốc độ tăng trưởng phần cứng máy tính 45%/năm và phần mềm 20%/năm, năm

2000 bán ra 10 triệu máy tính tại thị trường trong nước, nhưng số gia đình có MTĐT còn đạt tỷ lệ thấp (cao nhất là tại Thượng hải đạt 6%, còn toàn Trung quốc chỉ là 1%). Tuy mới vào Internet cuối 1997, nhưng năm 2000 Trung quốc đã đạt hơn 20 triệu thuê bao Internet, và dự kiến hoà mạng Internet cho 80% chính quyền địa phương, 80% công ty. Hiện chi phí sử dụng Internet ở đây còn quá cao (chiếm khoảng 10% thu nhập của người sử dụng so với 1% ở Mỹ), nên chưa có công bố tổng thể về doanh thu của TMĐT.

Trong khối ASEAN  Singapore có mục tiêu biến nước mình thành "hòn đảo thông minh" và là nước đứng hàng đầu thế giới về máy tính hoá. Singapore là một trong những nước áp dụng đầu tiên trên thế giới hình thức thanh toán điện tử. Theo kế hoạch của Chính phủ, năm 2001 giao dịch qua TMĐT sẽ đạt 16 tỷ USD và năm 2003 trong số 2,3 triệu dân Singapore sẽ có khoảng 1,5 triệu người dùng Internet.

Các nước ASEAN có hoạt động tập thể về TMĐT từ 1997 (Hội nghị bàn tròn ASEAN về TMĐT ở Malaisia tháng 10 năm 1997) và đã lập "Tiểu ban điều phối về TMĐT tháng 7/1998. 10/2000 lãnh đạo của 10 quốc gia thành viên ASEAN đã ký Hiệp định khung về TMĐT khẳng định quyết tâm của các nước ASEAN về thu hẹp khoảng cách phát triển trong khối về công nghệ thông tin.

Do sự phát triển còn khác nhau về công nghệ thông tin trong các nước thành viên, trong đó một số nước còn trong tình trạng yếu kém về cơ sở hạ tầng, cả về tài chính, pháp lý, nên còn có xu thế dè dặt trong phát triển TMĐT.

## 3. TÌNH HÌNH PHÁT TRIỂN TMĐT Ở VIỆT NAM.

Kể từ 19.11.1997 đến 11.2001, sau 4 năm kết nối Internet, Việt nam có 140.000 thuê bao Internet. Theo dự báo của Chính phủ, đến năm 2005 nước ta sẽ đạt bình quân 1,3 đến 1,5 thuê bao Internet/100 dân, tỷ lệ dân sử dụng Internet sẽ là 4 đến 5% (Báo Tiền phong số 44 ngày 1/3/2002). Theo kết quả khảo sát của Ban điều hành Dự án Kỹ thuật TMĐT Bộ Thương mại tại 56.000 doanh nghiệp, trong đó có 6.000 doanh nghiệp nhà nước, chỉ có 7% số doanh nghiệp quan tâm và bắt đầu triển khai TMĐT, 90% chưa có chút khái niệm nào về TMĐT. 1500 doanh nghiệp Việt nam có trang Web riêng, vài nghìn có trang Web quảng cáo. Rất ít doanh nghiệp Việt nam chủ động tạo website, phần lớn phải có sự thuyết phục của ISP. 48% doanh nghiệp Việt nam sử dụng Internet chỉ để nhận gửi email, 33% có kết nối Internet nhưng không dùng nó để hỗ trợ cho việc kinh doanh, 50% doanh nghiệp chỉ có 4 người biết sử dụng email. Như vậy, nếu xét về tất cả các mặt, hiện nay ***môi trường đúng nghĩa cho TMĐT ở Việt nam chưa hình thành***.

Lãnh đạo Đảng và Nhà nước Việt nam đã thể hiện quyết tâm thúc đẩy ngành công nghệ thông tin ( CNTT ) phát triển, đã có hàng loạt chỉ thị nghị quyết nhằm động viên thúc đẩy và tạo điều kiện cho CNTT phát triển. Chính phủ đã ban hành nghị định 49/CP ngày 04/8/1993 về phát triển CNTT ở VN trong những năm 90. Ngày 7/4/1995 Chính phủ ra quyết định số 211/TTg phê duyệt kế hoạch tổng thể về phát

triển CNTT Việt Nam cho đến năm 2000. Chính phủ đã có quyết định số 212/TTg ngày 6/5/1994 và quyết định số 154/TTg ngày 11/3/1995 về thành lập Ban chỉ đạo Chương trình Quốc gia về CNTT. Ban chỉ đạo đã triển khai hoạt động giai đoạn 1996-1999. Ngày 11/5/1999 Chính phủ ra quyết định số 123/1999/QĐ-TTg thành lập Ban chỉ đạo Chương trình Kỹ thuật-Kinh tế về CNTT; Quyết định số 192/1999/QĐ-TTg ngày 20/9/1999 giải thể Ban chỉ đạo Quốc gia về CNTT. Ngày 5/6/2000 Chính phủ ban hành Nghị quyết số 07/2000/NQ-CP về xây dựng và phát triển công nghiệp phần mềm giai đoạn 2000-2005. Tháng 10/2000 Bộ Chính trị ra Chỉ thị 58CT/TƯ về đẩy mạnh ứng dụng phát triển CNTT phục vụ sự nghiệp công nghiệp hoá hiện đại hoá. Tháng 11/2000 Thủ tướng ra quyết định 128/2000/QĐ-TTg về một số chính sách và biện pháp khuyến khích đầu tư và phát triển công nghệ phần mềm. Ngày 23/8/2001 Chính phủ ban hành nghị định số 55/2001/NĐ-CP về quản lý, cung cấp và sử dụng dịch vụ Internet.

Trong năm 2000 và 2001, đã có nhiều hội thảo về TMĐT được tổ chức tại VN.

Ban TMĐT Bộ thương mại đã triển khai dự án quốc gia về kỹ thuật TMĐT. Dự án gồm nhiều tiểu dự án: Phát triển nâng cao nhận thức về TMĐT, Bảo hộ trí tuệ và người tiêu dùng, Nghiên cứu về các khía cạnh xã hội liên quan, Vai trò Nhà nước và quản lý của Chính phủ trong TMĐT, Về cơ sở hạ tầng cho TMĐT,...Các ngành tài chính và ngân hàng đã chuyển dần phương pháp giao dịch giữa người và người sang người và máy, máy và máy, đó cũng là những bước đi quan trọng cho phát triển TMĐT.

Ngoài cơ sở hạ tầng về CNTT, luật TMĐT ở VN chưa hình thành nên thực chất cho đến nay chưa hình thành được một khung pháp lý trong kinh doanh điện tử và TMĐT.

Trong hoàn cảnh Việt nam, khi thói quen dùng tài khoản cá nhân và những dịch vụ liên quan chưa được tạo ra, khi xem tận mắt hàng hoá còn chưa dám khẳng định mức độ thật, khi pháp lý còn chưa được xây dựng hoàn chỉnh, các hoạt động tự do thiếu tôn trọng pháp luật diễn ra còn phổ biến, thì việc phát triển thương mại điện tử đương nhiên sẽ gặp nhiều khó khăn. Tuy vậy, nếu thấy hết được những ưu việt to lớn của TMĐT, thì vẫn phải xúc tiến nhanh những công việc liên quan để TMĐT đi vào cuộc sống , góp phần tích cực cho việc tăng trưởng kinh tế và hoà nhập với thế giới.

## 4. AN TOÀN TRONG TMĐT.

An toàn thông tin và an toàn hệ thống là những vấn đề hết sức quan trọng trong TMĐT. Vấn đề an toàn hệ thống không chỉ quan trọng trong kinh tế , mà còn có vai trò rất lớn trong an ninh quốc gia. Khi lợi ích kinh tế bị xâm hại nghiêm trọng, thì an toàn an ninh quốc gia sẽ không thể đảm bảo được. Công cụ càng hiện đại khi bị dùng vào mục đích xấu thì thiệt hại gây ra cho quốc gia càng lớn.

### 4.1. Các mối đe doạ đến sự an toàn của TMĐT

- *Truy cập và khai thác thông tin không hợp pháp*. Những thông tin nhạy cảm như các báo cáo tài chính, số thẻ tín dụng của khách hàng, danh sách địa chỉ giao dịch,... đều dễ bị khai thác trái phép. theo một kết quả điều tra 70% các cuộc truy cập không hợp pháp thường do những nhân viên công ty, những người quản trị hệ thống tiến hành, tức là những người trong nội bộ công ty tiến hành.
- *Chặn thu hoặc đánh cắp thông tin*. Có thể chặn thu thông tin trên đường truyền để khai thác trái phép hoặc đánh cắp trong quá trình lưu trữ, xử lý.
- *Thao tác sửa đổi, thêm bớt dữ liệu một cách bất hợp pháp*: Trong cạnh tranh các đối tác có thể dùng mọi thủ đoạn để làm mất uy tín công ty dẫn đến việc mất khách hàng. Sửa đổi dữ liệu sẽ dẫn đến những sai sót tai hại trong xử lý.
- *Làm gián đoạn giao dịch hoặc từ chối dịch vụ*: dẫn đến những hành động ngăn ngừa người dùng truy nhập dữ liệu hoặc sử dụng tài nguyên.
- *Huỷ thông tin của đối tác*, *phá huỷ hệ thống*.

Những mối đe doạ (hiểm hoạ) có thể được phân thành hai lớp: *có chủ ý* và *vô tình*.

Những hiểm hoạ mang tính ngẫu nhiên hay hiểm hoạ vô tình là những biến cố thông thường độc lập với những điều khiển gây ra sự phá hỏng thông tin, chúng thường liên quan đến các trường hợp sau:

- Những thảm hoạ mang tính ngẫu nhiên như động đất, hoả hoạn, lụt lội... Những yếu tố ngẫu nhiên đó có thể làm hỏng hệ thống phần cứng của hệ thống, hệ thống số liệu lưu giữ. Những hiểm hoạ này luôn gây ra sự vi phạm về tính toàn vẹn của dữ liệu hoặc từ chối dịch vụ.
- Các lỗi phần mềm hay phần cứng có thể dẫn đến việc áp dụng các chính sách an toàn một cách không chính xác và có thể sẽ dẫn đến việc truy nhập, đọc, sửa đổi dữ liệu một cách bất hợp pháp hay từ chối phục vụ những người dùng hợp pháp.
- Những sai phạm do con người gây ra  những vi phạm không cố ý như là việc nhập đầu vào không chính xác, hay sử dụng các ứng dụng không chính xác, hậu quả cũng tương tự như những nguyên nhân lỗi phần mềm hay lỗi kỹ thuật gây ra.

Những yếu tố mang tính chất cố ý là những can thiệp mang tính chất cố tình gây nên nguyên nhân phá hỏng hệ thống thông tin cần bảo mật. Những vi phạm trên liên quan đến hai lớp người dùng như sau:

1. Những người dùng được phép: là những người có thể lạm quyền, sử dụng vượt quá quyền hạn được phép của họ.

2. Bên chống đối: là những người, những nhóm người truy cập thông tin một cách trái phép, bao gồm những người nằm ngoài tổ chức hay bên trong tổ chức. Họ tiến hành những hành vi phá hoại phần mềm CSDL hay phần cứng của hệ thống, hoặc đọc ghi dữ liệu trái phép. Trong cả hai trường hợp trên họ thực hiện với chủ đích rõ ràng. Đặc biệt với những chương trình như *con ngựa thành Tơ roa* và các cửa sập là những kiểu tấn công bên địch. Virus là một đoạn mã chương trình có

thể tự động sao chép lại chính nó và gây hư hỏng lâu dài, thông thường không sửa chữa được môi trường nơi mà virus đã sinh sôi.

### 4.2. Những yêu cầu bảo vệ thông tin và các giải pháp đảm bảo an toàn thông tin

Bảo vệ thông tin là bảo vệ các tài nguyên, đặc biệt là bảo vệ dữ liệu khỏi những thảm hoạ hay những truy nhập bất hợp pháp. Những yêu cầu của bảo vệ có thể tóm tắt như sau:

**-** *Bảo vệ khỏi những truy nhập không được phép*

Đây là một vấn đề cơ bản bao gồm trao quyền truy nhập cho những người dùng được quyền truy nhập. Những yêu cầu truy nhập phải được kiểm tra kiểm soát. Việc kiểm soát cần phải áp cho các đối tượng như các bản ghi, các thuộc tính và các giá trị.

**-** *Bảo vệ khỏi những suy luận*

Suy luận chỉ ra khả năng có được các thông tin bí mật từ những thông tin không mang tính bí mật. Đặc biệt những vấn đề suy luận có thể suy ra từ những dữ liệu thống kê.

**-** *Bảo vệ tính toàn vẹn của thông tin*

Yêu cầu này liên quan vấn đề bảo vệ khỏi những truy nhập trái phép có thể dẫn đến thay đổi nội dung dữ liệu cũng như khỏi những lỗi, virus, hỏng hóc trong hệ thống có thể gây hỏng dữ liệu. Thông tin quan trọng thường phải dùng đến những phương pháp bảo vệ đặc biệt như mã hoá, xác thực nội dung, xác thực nguồn gốc bằng những phương pháp mật mã. Một cách bảo vệ khác là thực hiện bằng những thủ tục sao lưu, phục hồi. Hệ thống cũng có thể sử dụng nhật ký. Với mỗi giao tác, nhật ký ghi lại các phép toán đã được thực hiện trên dữ liệu (read, write, delete, insert). Hệ thống phục hồi đọc file nhật ký để xác định giáo tác nào bị huỷ bỏ và giao tác nào cần phải thực hiện lại. Với những giao dịch trong nội bộ công ty có thể dùng mạng riêng ảo.

**-** *Xác thực người dùng và cấp phép*

Người dùng được phép truy nhập dữ liệu khi đã được cấp phép và xác định là những người dùng hợp pháp bởi hệ thống. Có nhiều phương pháp xác thực người dùng từ đơn giản đến phức tạp như yêu cầu tên, mật khẩu, dùng chứng chỉ số, chữ ký số, xác thực nội dung thông tin bằng các phương pháp mật mã.

**-** *Quản lý và bảo vệ dữ liệu nhạy cảm*

Dữ liệu nhạy cảm là những dữ liệu không nên đưa ra trước công chúng. Kiểm soát truy nhập cũng cho phép người dùng đã được trao quyền trên dữ liệu nhậy cảm có thể làm việc với dữ liệu không nhậy cảm cùng với những người dùng khác mà không gây trở ngại nào.

**-** *Bảo vệ nhiều mức*

Các thông tin có thể được phân loại thành nhiều mức khác nhau. Trong tình trạng này, bảo vệ nhiều mức nhằm mục đích phân loại các mức độ khác nhau của các thông tin khác nhau và cũng để phân quyền cho các mức độ truy cập khác nhau tới những thông tin riêng biệt theo sự phân loại của chúng. Hiện nay để bảo vệ nhiều mức người ta đã đưa ra các giải pháp phổ dụng như dùng bức tường lửa, dùng các thiết bị mã luồng, các biện pháp bảo vệ cơ sở dữ liệu,...

*-Các chính sách an toàn*

Các chính sách an toàn định nghĩa những nguyên tắc mà dựa vào đó việc truy nhập sẽ được chấp nhận hoặc bị từ chối. Như chúng ta đã biết, an toàn thông tin bao gồm: (1) *Mức ngoài*, nghĩa là kiểm soát truy nhập vật lý đến hệ thống xử lý và bảo vệ hệ thống xử lý khỏi những thảm hoạ do tự nhiên, con người hoặc máy móc gây ra. (2) *Mức trong*, chống lại những tấn công có thể có trên hệ thống từ sự gian lận hoặc không có tư cách và những lỗi của những người trong và bên ngoài hệ thống.

Nhìn chung, những yêu cầu bảo vệ của hệ thống liên quan chặt chẽ đến môi trường nơi hệ thống được sử dụng, với những cân nhắc cụ thể về lợi ích kinh tế của chúng. Những đặc thù an toàn kéo theo chi phí phát sinh và nguyên nhân giảm hiệu suất. Các biện pháp an toàn còn dẫn đến sự phức tạp hệ thống: làm mất đi tính mềm dẻo; nhu cầu về nguồn nhân lực thiết kế, quản lý và duy tu; cũng như nhu cầu về phần mềm và phần cứng phát sinh. Có sự khác biệt giữa yêu cầu an toàn của các hệ thống thông tin thương mại và hệ thống thông tin của chính phủ, thông tin trong an ninh quốc phòng.

Những chính sách và biện pháp đảm bảo an toàn có thể gọi chung là chiến lược an toàn. Nói chung sẽ không có một giải pháp nào bảo đảm an toàn tuyệt đối trên Internet phù hợp với mọi đối tượng. Tuy vậy an toàn của hệ thống phụ thuộc rất nhiều vào chiến lược an toàn mà chúng ta chọn ngay từ khi bắt đầu xây dựng hệ thống.

### 4.3. Một số khuyến nghị trên con đường tiến tới TMĐT ở Việt Nam

Theo một số tài liệu và ý kiến của các chuyên gia nước ngoài , để tiến tới TMĐT ở VN,

*Chính phủ cần phải:*

- Hiểu được sự cấp thiết khởi động TMĐT.
- Hiểu rằng không cần thiết phải điều tiết tất cả mọi thứ trước khi TMĐT có thể được tiến hành. Tại hầu hết các quốc gia trên thế giới TMĐT ra đời trước khi bất cứ đạo luật nào được ban hành.
- Việc áp dụng đơn thuần những kinh nghiệm TMĐT từ những nước khác vào VN là chưa đủ vì Việt nam còn tồn tại những luật lệ và thủ tục hành chính riêng.
- Hiểu rằng chỉ cần một vài điều chỉnh quy mô nhỏ là đủ để tiến hành những ứng dụng TMĐT ở VN trong thời gian đầu.

*Cộng đồng doanh nghiệp cần phải:*

- Hiểu rằng họ không thể và không phải đợi những đạo luật, quy định thật cụ thể của Chính phủ để tiến hành TMĐT.
- Hiểu được lợi ích của các thủ tục mới trong kinh doanh khi công nghệ thông tin phát triển.
- Hiểu rằng TMĐT có thể thúc đẩy sự phát triển và phải tiến hành sớm khi chưa để mất thị phần trên thị trường thế giới vào tay các nước khác.
- Có thể phải chấp nhận rủi ro ở mức hạn chế khi áp dụng TMĐT.

## TÀI LIỆU THAM KHẢO


1) Tạp chí Bưu chính viễn thông, kỳ 2, tháng 1/ 2002.
2) Thương mại điện tử. NXB Giao thông vận tải, Hà Nội - 2001.
3) Tin nhanh tuần, Ban CYCP.
4) Tin trên các báo hàng ngày của Việt Nam.
5) Một số bản tin điện tử trên Internet.