CHƯƠNG 1: GIỚI THIỆU

Mục đích: *Giới thiệu chung về các khái niệm cơ bản trong An toàn thông tin và an toàn mạng. Các yếu tố xác lập an toàn thông tin. Mô hình an toàn mạng.*

Yêu cầu: *Sinh viên nắm được các khái niệm cơ bản về an toàn thông tin và an toàn mạng. Hiểu rõ các yếu tố xác lập an toàn thông tin và vẽ được mô hình an toàn mạng.*

1.1 Giới thiệu

Trước đây khi công nghệ máy tính chưa phát triển, khi nói đến vấn đề an toàn bảo mật thông tin (Information Security), chúng ta thường hay nghĩ đến các biện pháp nhằm đảm bảo cho thông tin được trao đổi hay cất giữ một cách an toàn và bí mật. Chẳng hạn là các biện pháp như:

- Đóng dấu và ký niêm phong một bức thư để biết rằng lá thư có được chuyển nguyên vẹn đến người nhận hay không.
- Dùng mật mã mã hóa thông điệp để chỉ có người gửi và người nhận hiểu được thông điệp. Phương pháp này thường được sử dụng trong chính trị và quân sự.
- Lưu giữ tài liệu mật trong các két sắt có khóa, tại các nơi được bảo vệ nghiêm ngặt, chỉ có những người được cấp quyền mới có thể xem tài liệu.

Với sự phát triển mạnh mẽ của công nghệ thông tin, đặc biệt là sự phát triển của mạng Internet, ngày càng có nhiều thông tin được lưu giữ trên máy vi tính và gửi đi trên mạng Internet. Và do đó xuất hiện nhu cầu về an toàn và bảo mật thông tin trên máy tính. Có thể phân loại mô hình an toàn bảo mật thông tin trên máy tính theo hai hướng chính như sau:

1) Bảo vệ thông tin trong quá trình truyền thông tin trên mạng (Network Security)

2) Bảo vệ hệ thống máy tính, và mạng máy tính, khỏi sự xâm nhập phá hoại từ bên ngoài (System Security)

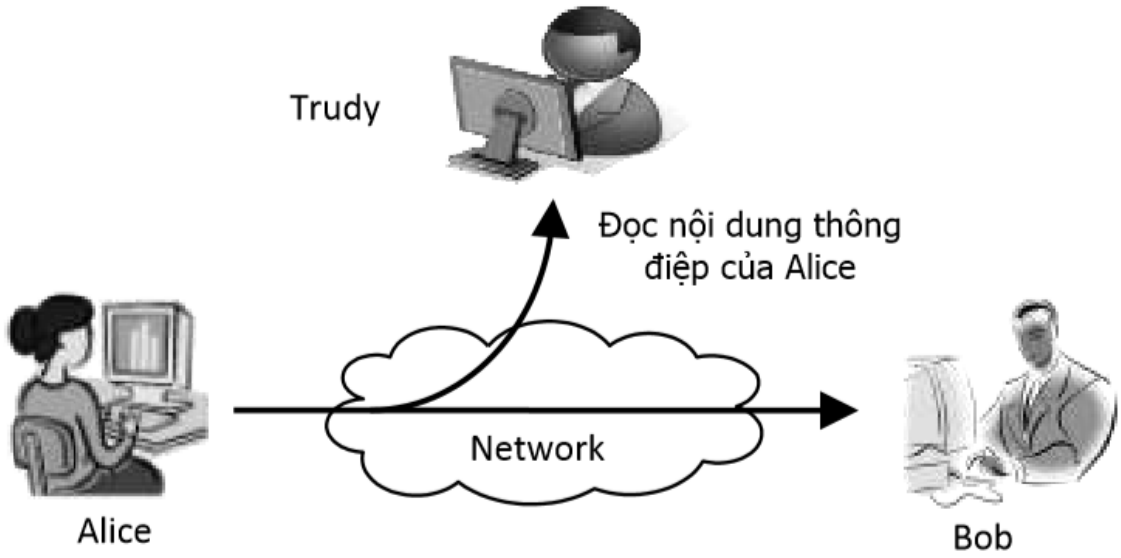
1.2 Bảo vệ thông tin trong quá trình truyền thông tin trên mạng

1.2.1 Các loại hình tấn công

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

1) Xem trộm thông tin (Release of Message Content)

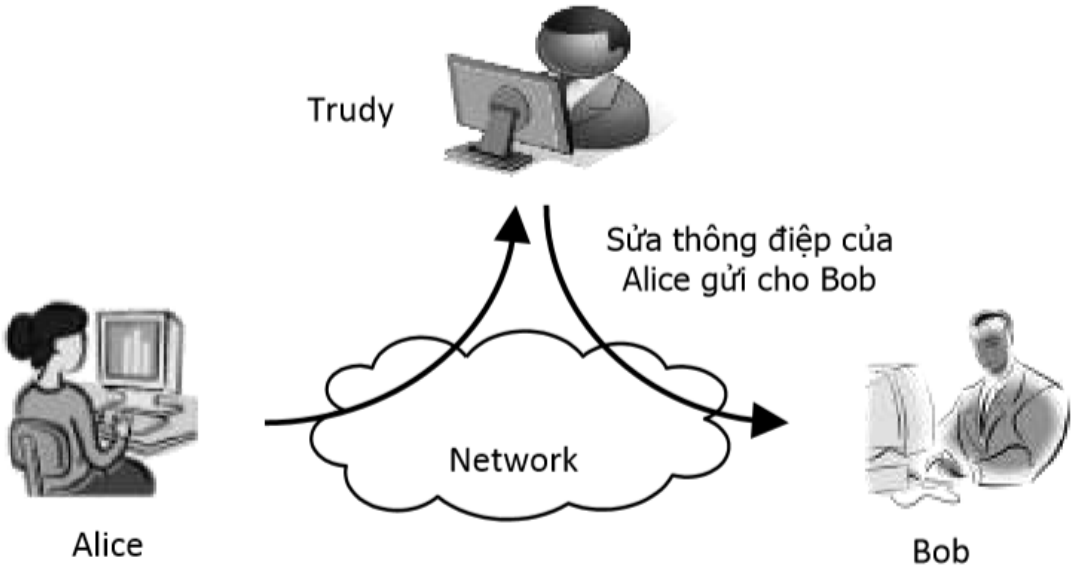
Trong trường hợp này Trudy chặn các thông điệp Alice gửi cho Bob, và xem được nội dung của thông điệp.



Hình 1-1. Xem trộm thông điệp

2) Thay đổi thông điệp (Modification of Message)

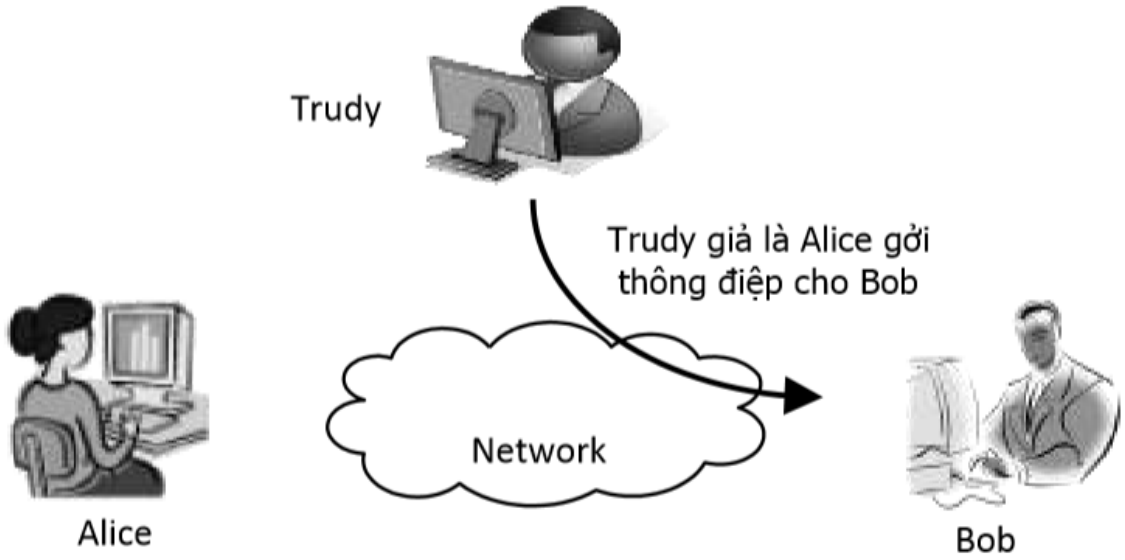
Trudy chặn các thông điệp Alice gửi cho Bob và ngăn không cho các thông điệp này đến đích. Sau đó Trudy thay đổi nội dung của thông điệp và gửi tiếp cho Bob. Bob nghĩ rằng nhận được thông điệp nguyên bản ban đầu của Alice mà không biết rằng chúng đã bị sửa đổi.



Hình 1-2. Sửa thông điệp

3) Mạo danh (Masquerade)

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

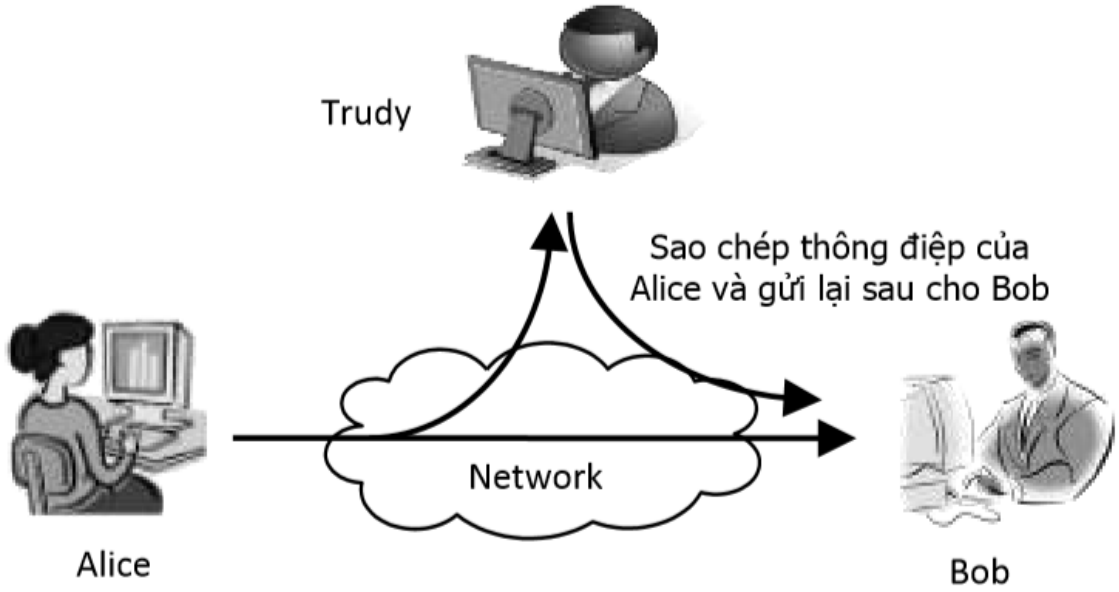


Hình 1-3. Mạo danh

4) Phát lại thông điệp (Replay)

Trudy sao chép lại thông điệp Alice gửi cho Bob. Sau đó một thời gian Trudy gửi bản sao chép này cho Bob. Bob tin rằng thông điệp thứ hai vẫn là từ

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



Hình 1-4. Phát lại thông điệp

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

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

1) Tính bảo mật (Confidentiality): Ngăn chặn được vấn đề xem trộm thông điệp.

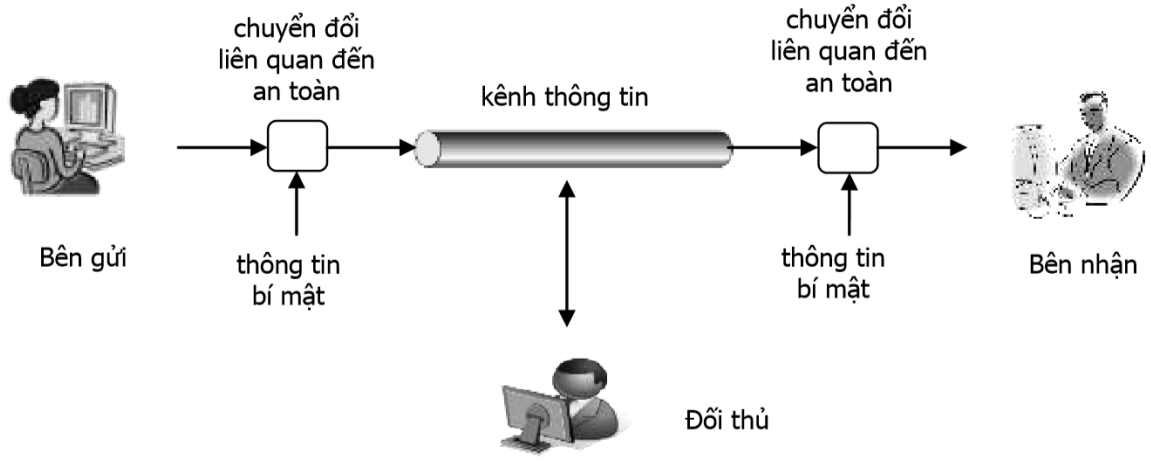
2) Tính chứng thực (Authentication): Nhằm đảm bảo cho Bob rằng thông điệp mà Bob nhận được thực sự được gửi đi từ Alice, và không bị thay đổi trong

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

3) Tính không từ chối (Nonrepudiation): xét tình huống sau:

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

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



Hình 1-5. Mô hình bảo mật truyền thông tin trên mạng

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

Mật mã hay mã hóa dữ liệu (cryptography), là một công cụ cơ bản thiết yếu của bảo mật thông tin. Mật mã đáp ứng được các nhu cầu về tính bảo mật (confidentiality), tính chứng thực (authentication) và tính không từ chối (non-repudiation) của một hệ truyền tin.

Tài liệu này trước tiên trình bày về mật mã cổ điển. Những hệ mật mã cổ điển này tuy ngày nay tuy ít được sử dụng, nhưng chúng thể hiện những nguyên lý cơ bản được ứng dụng trong mật mã hiện đại. Dựa trên nền tảng đó, chúng ta sẽ tìm hiểu về mã hóa đối xứng và mã hóa bất đối xứng, chúng đóng vai trò quan

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

1.2.4 Các giao thức (protocol) thực hiện bảo mật.

Sau khi tìm hiểu về mật mã, chúng ta sẽ tìm hiểu về cách ứng dụng chúng vào thực tế thông qua một số giao thức bảo mật phổ biến hiện nay là:

- Keberos: là giao thức dùng để chứng thực dựa trên mã hóa đối xứng.
- Chuẩn chứng thực X509: dùng trong mã hóa khóa công khai.
- Secure Socket Layer (SSL): là giao thức bảo mật Web, được sử dụng phổ biến trong Web và thương mại điện tử.
- PGP và S/MIME: bảo mật thư điện tử email.

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

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

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

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

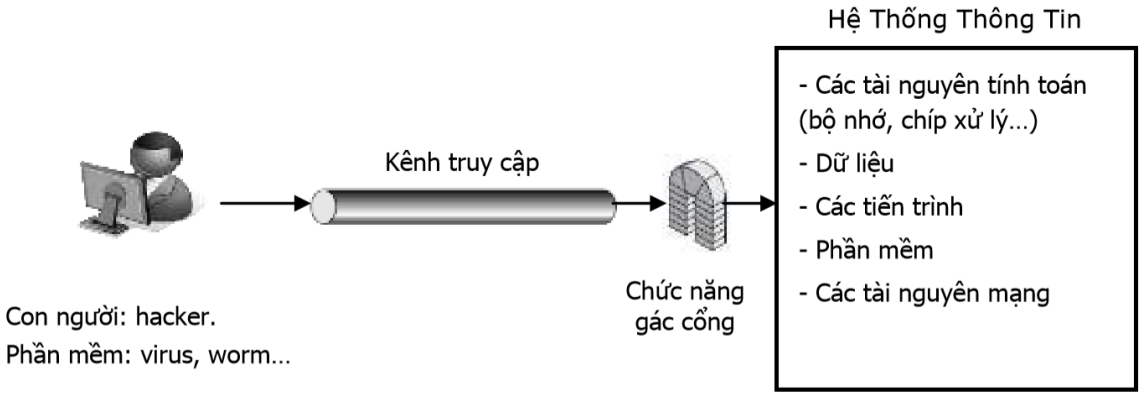
vào hệ điều hành, tuy nhiên bạn chỉ được cấp quyền để đọc một file nào đó. Hoặc bạn chỉ có quyền đọc file mà không có quyền xóa file.

Với nguyên tắc như vậy thì một máy tính hoặc một mạng máy tính được bảo vệ khỏi sự thâm nhập của các đối tượng không được phép. Tuy nhiên thực tế chúng ta vẫn nghe nói đến các vụ tấn công phá hoại. Để thực hiện điều đó, kẻ phá hoại tìm cách phá bỏ cơ chế Authentication và Authorization bằng các cách thức sau:

- Dùng các đoạn mã phá hoại (Malware): như virus, worm, trojan, backdoor… những đoạn mã độc này phát tán lan truyền từ máy tính này qua máy tính khác dựa trên sự bất cẩn của người sử dụng, hay dựa trên các lỗi của phần mềm. Lợi dụng các quyền được cấp cho người sử dụng (chẳng hạn rất nhiều người login vào máy tính với quyền administrator), các đoạn mã này thực hiện các lệnh phá hoại hoặc dò tìm password của quản trị hệ thống để gửi cho hacker, cài đặt các cổng hậu để hacker bên ngoài xâm nhập.
- Thực hiện các hành vi xâm phạm (Intrusion): việc thiết kế các phần mềm có nhiều lỗ hổng, dẫn đến các hacker lợi dụng để thực hiện những lệnh phá hoại. Những lệnh này thường là không được phép đối với người bên ngoài, nhưng lỗ hổng của phần mềm dẫn đến được phép. Trong những trường hợp đặc biệt, lỗ hổng phần mềm cho phép thực hiện những lệnh phá hoại mà ngay cả người thiết kế chương trình không ngờ tới. Hoặc hacker có thể sử dụng các cổng hậu do các backdoor tạo ra để xâm nhập.

Để khắc phục các hành động phá hoại này, người ta dùng các chương trình có chức năng gác cổng, phòng chống. Những chương trình này dò tìm virus hoặc dò tìm các hành vi xâm phạm đển ngăn chặn chúng, không cho chúng thực hiện hoặc xâm nhập.

Đó là các chương trình chống virus, chương trình firewall… Ngoài ra các nhà phát triển phần mềm cần có quy trình xây dựng và kiểm lỗi phần mềm nhằm hạn chế tối đa những lỗ hổng bảo mật có thể có.



Hình 1-6.Mô hình phòng chống xâm nhập và phá hoại hệ thống

1.4 Mô hình an toàn mạng

1.4.1 Kiến trúc an toàn của hệ thống truyền thông mở OSI.

Để giúp cho việc hoạch định chính sách và xây dựng hệ thống an ninh tốt. Bộ phận chuẩn hóa tiêu chuẩn của tổ chức truyền thông quốc tế (International Telecommunication Union) đã nghiên cứu và đề ra Kiến trúc an ninh X800 dành cho hệ thống trao đổi thông tin mở OSI. Trong đó định nghĩa một cách hệ thống phương pháp xác định và cung cấp các yêu cầu an toàn. Nó cung cấp cho chúng ta một cách nhìn tổng quát, hữu ích về các khái niệm mà chúng ta nghiên cứu.

Trước hết nói về dịch vụ an toàn, X800 định nghĩa đây là dịch vụ cung cấp cho tầng giao thức của các hệ thống mở trao đổi thông tin, mà đảm bảo an toàn thông tin cần thiết cho hệ thống và cho việc truyền dữ liệu.

Trong tài liệu các thuật ngữ chuẩn trên Internet RFC 2828 đã nêu định nghĩa cụ thể hơn dich vụ an toàn là dịch vụ trao đổi và xử lý cung cấp cho hệ thống việc bảo vệ đặc biệt cho các thông tin nguồn.Tài liệu X800 đưa ra định nghĩa dịch vụ theo 5 loại chính:

- Xác thực: tin tưởng là thực thể trao đổi đúng là cái đã tuyên bố. Người đang trao đổi xưng tên với mình đúng là anh ta, không cho phép người khác mạo danh.

- Quyền truy cập: ngăn cấm việc sử dụng nguồn thông tin không đúng vai trò. Mỗi đối tượng trong hệ thống được cung cấp các quyền hạn nhất định và chỉ được hành động trong khuôn khổ các quyền hạn đó.
- Bảo mật dữ liệu: bảo vệ dữ liệu không bị khám phá bởi người không có quyền. Chẳng hạn như dùng các ký hiệu khác để thay thế các ký hiệu trong bản tin, mà chỉ người có bản quyền mới có thể khôi phục nguyên bản của nó.
- Toàn vẹn dữ liệu: tin tưởng là dữ liệu được gửi từ người có quyền. Nếu có thay đổi như làm trì hoãn về mặt thời gian hay sửa đổi thông tin, thì xác thực sẽ cho cách kiểm tra nhận biết là có các hiện tượng đó đã xảy ra.
- Không từ chối: chống lại việc chối bỏ của một trong các bên tham gia trao đổi. Người gửi cũng không trối bỏ là mình đã gửi thông tin với nội dung như vậy và người nhận không thể nói dối là tôi chưa nhận được thông tin đó. Điều này là rất cần thiết trong việc trao đổi, thỏa thuận thông tin hàng ngày.

Cơ chế an toàn được định nghĩa trong X800 như sau:

- Cơ chế an toàn chuyên dụng được cài đặt trong một giao thức của một tầng vận chuyển nào đó: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, đệm truyền, kiểm soát định hướng, công chứng.
- Cơ chế an toàn phổ dụng không chỉ rõ được dùng cho giao thức trên tầng nào hoặc dịch vụ an ninh cụ thể nào: chức năng tin cậy cho một tiêu chuẩn nào đó, nhãn an toàn chứng tỏ đối tượng có tính chất nhất định, phát hiện sự kiện, vết theo dõi an toàn, khôi phục an toàn.

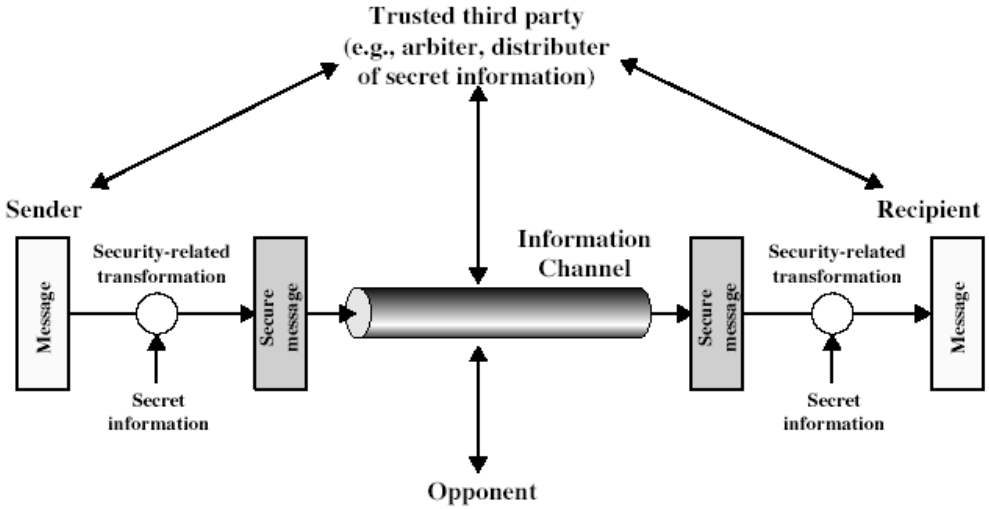
1.4.2 Mô hình an toàn mạng tổng quát

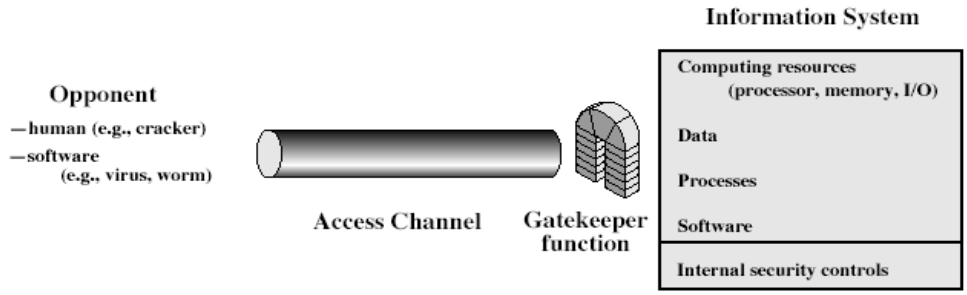
Sử dụng mô hình trên đòi hỏi chúng ta phải thiết kế:

- Thuật toán phù hợp cho việc truyền an toàn.
- Phát sinh các thông tin mật (khoá) được sử dụng bởi các thuật toán.
- Phát triển các phương pháp phân phối và chia sẻ các thông tin mật.

- Đặc tả giao thức cho các bên để sử dụng việc truyền và thông tin mật cho các dịch vụ an toàn.

Mô hình truy cập mạng an toàn:





Sử dụng mô hình trên đòi hỏi chúng ta phải:

- Lựa chọn hàm canh cổng phù hợp cho người sử dụng có danh tính.
- Cài đặt kiểm soát quyền truy cập để tin tưởng rằng chỉ có người có quyền mới truy cập được thông tin đích hoặc nguồn.
- Các hệ thống máy tính tin cậy có thể dùng mô hình này.