TRƯỜNG ĐẠI HỌC GIAO THÔNG
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN KHOA HỌC MÁY TÍNH
Biên soạn TS. Trần Văn Dũng

GIÁO TRÌNH

AN TOÀN VÀ BẢO MẬT THÔNG TIN

Hà nội 8-2007

Mở đầu

Gần đây, môn học "An toàn và bảo mật thông tin" đã được đưa vào giảng dạy tại hầu hết các Khoa Công nghệ Thông tin của các trường đại học và cao đẳng. Do các ứng dụng trên mạng Internet ngày các phát triển và mở rộng, nên an toàn thông tin trên mạng đã trở thành nhu cầu bắt buộc cho mọi hệ thống ứng dụng. Để đáp ứng yêu cầu học tập và tự tìm hiểu của sinh viên các chuyên ngành Công nghệ Thông tin, Bộ môn Khoa học máy tính, Khoa Công nghệ Thông tin, trường đại học Giao thông đã tổ chức biên soạn giáo trình này. Nội dung của nó được dựa trên một số tài liệu, nhưng chủ yếu là cuốn sách của Giáo sư William Stallings "Cryptography and Network Security: Principles and Practice". Cuốn sách trên đã được dùng làm tài liệu giảng dạy tại nhiều trường đại học. Đồng thời giáo trình này cũng được hoàn thiện từng bước dựa trên bài giảng của tác giả cho 4 khóa sinh viên Khoa Công nghệ Thông tin vừa qua. Với mục đích trang bị các kiến thức cơ sở vừa đủ và giúp cho sinh viên hiểu được bản chất của các khía cạnh an ninh trên mạng, trong giáo trình tác giả đã cố gắng trình bày tóm tắt các phần lý thuyết cơ bản và đưa ra các ứng dụng thực tế.

Giáo trình gồm 8 chương. Chương đầu nêu tổng quan về bảo mật, chương 2 tóm tắt sơ lược về mã cổ điển, chương 3 trình bày những khái niệm cơ bản về trường số học, chương 4 giới thiệu về mã khối và chuẩn mã dữ liệu, chương 5 nêu về mã công khai và RSA, chương 6 đưa ra khái niệm xác thực và hàm băm, chương 7 giới thiệu ứng dụng về an toàn Web và IP và cuối cùng chương 8 tóm tắt về kẻ xâm nhập và biện pháp phòng chống bức tường lửa.

Do lần đầu biên soạn và chưa có nhiều kinh nghiệm thực tế, nên không tránh khỏi những sai sót và lỗi in ấn nhất định. Tác giả xin vui lòng tiếp nhận mọi sự đóng góp giúp cho giáo trình "An toàn và bảo mật thông tin" ngày càng tốt hơn. Mọi ý kiến xây dựng xin gửi về theo địa chỉ sau: Trần Văn Dũng, Khoa Công nghệ Thông tin, Đại học Giao thông Vận tải, Láng Thượng, Đống đa, Hà nội.

MỤC LỤC

TRƯỜNG ĐAI HOC GIAO THÔNG
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN KHOA HỌC MÁY TÍNH.....1
Biên soan TS. Trần Văn Dũng 1
GIÁO TRÌNH.....1
AN TOÀN VÀ BẢO MẬT THÔNG TIN.....1
Hà nội 8-2007.....1
Mở đầu 2
Gần đây, môn học "An toàn và bảo mật thông tin" đã được đưa vào giảng dạy tại hầu hết các Khoa Công nghệ Thông tin của các trường đại học và cao đẳng. Do các ứng dụng trên mạng Internet ngày các phát triển và mở rộng, nên an toàn thông tin trên mạng đã trở thành nhu cầu bắt buộc cho mọi hệ thống ứng dụng. Để đáp ứng yêu cầu học tập và tự tìm hiểu của sinh viên các chuyên ngành Công nghệ Thông tin, Bộ môn Khoa học máy tính, Khoa Công nghệ Thông tin, trường đại học Giao thông đã tổ chức biên soạn giáo trình này. Nội dung của nó được dựa trên một số tài liệu, nhưng chủ yếu là cuốn sách của Giáo sư William Stallings "Cryptography and Network Security: Principles and Practice". Cuốn sách trên đã được dùng làm tài liệu giảng dạy tại nhiều trường đại học. Đồng thời giáo trình này cũng được hoàn thiện từng bước dựa trên bài giảng của tác giả cho 4 khóa sinh viên Khoa Công nghệ Thông tin vừa qua. Với muc đích trang bi các kiến thức cơ sở vừa đủ và giúp cho sinh viên hiểu được bản chất của các khía canh an ninh trên mang, trong giáo trình tác giả đã cố gắng trình bày tóm tắt các phần lý thuyết cơ bản và đưa ra các ứng dụng thực tế. 2
Do lần đầu biên soạn và chưa có nhiều kinh nghiệm thực tế, nên không tránh khỏi những sai sót và lỗi in ấn nhất đinh. Tác giả xin vui lòng tiếp nhận mọi sư đóng góp giúp cho giáo trình "An toàn và bảo mật thông tin" ngày càng tốt hơn. Mọi ý kiến xây dưng xin gửi về theo đia chỉ sau: Trần Văn Dũng, Khoa Công nghệ Thông tin, Đai hoc Giao thông Vận tải, Láng Thượng, Đống đa, Hà nội.....2
2

.....4
CHƯƠNG I.....5
TỔNG QUAN VỀ BẢO MẬT.....5
I.1 Giới thiệu chung về bảo mật thông tin.....5
I.3 Mô hình an toàn mạng.....8
I.4 Bảo mật thông tin trong hệ cơ sở dữ liệu.....10
MÃ CỔ ĐIỂN.....14
MEMATRHTGPRYETEFETEOAAT.....24
Thuật toán Miller - Rabin 40
CHUẨN MÃ DỮ LIỆU (DES) VÀ CHUẨN MÃ NÂNG CAO (AES).....45
Sinh số ngẫu nhiên tự nhiên: 72
Ví du 79
Ví du: 85
Các mã xác thực mẩu tin MAC cung cấp sự tin cậy cho người nhận là mẩu tin không bi thay đổi và từ đích danh người gửi. Cũng có thể sử dụng mã xác thực MAC kèm theo với việc mã hoá để bảo mật. Nói chung người ta sử dụng các khoá riêng biệt cho mỗi MAC và có thể tính MAC trước hoặc sau mã hoá, tốt hơn là thực hiện MAC trước và mã hoá sau. 92
Các tính chất của MAC.....92
Các tính chất của hàm Hash.....93
Các yêu cầu của hàm Hash.....94
Tấn công ngày sinh nhật 94
Toàn ven dữ liêu.....108
DANH MUC CÁC KÝ HIÊU, CÁC CHỮ VIẾT TẮT.....147

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT.....

Phụ lục 145

CHƯƠNG I
TỔNG QUAN VỀ BẢO MẬT

I.1 Giới thiệu chung về bảo mật thông tin

I.1.1 Mở đầu về bảo mật thông tin

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên,…đều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của doanh nghiệp là những đòi hỏi ngày càng cao của môi trường kinh doanh yêu cầu doanh nghiệp cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua Internet hay Intranet. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng của công ty và quan hệ với khách hàng.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của doanh nghiệp. Vì vậy an toàn và bảo mật thông tin là nhiệm vụ rất nặng nề và khó đoán trước được, nhưng tựu trung lại gồm ba hướng chính sau:

- Bảo đảm an toàn thông tin tại máy chủ
- Bảo đảm an toàn cho phía máy trạm
- Bảo mật thông tin trên đường truyền

Đứng trước yêu cầu bảo mật thông tin, ngoài việc xây dựng các phương thức bảo mật thông tin thì người ta đã đưa ra các nguyên tắc về bảo vệ dữ liệu như sau:

- Nguyên tắc hợp pháp trong lúc thu thập và xử lý dữ liệu.
- Nguyên tắc đúng đắn.
- Nguyên tắc phù hợp với mục đích.
- Nguyên tắc cân xứng.
- Nguyên tắc minh bạch.
- Nguyên tắc được cùng quyết định cho từng cá nhân và bảo đảm quyền truy cập cho người có liên quan.
- Nguyên tắc không phân biệt đối xử.
- Nguyên tắc an toàn.
- Nguyên tắc có trách niệm trước pháp luật.
- Nguyên tắc giám sát độc lập và hình phạt theo pháp luật.
- Nguyên tắc mức bảo vệ tương ứng trong vận chuyển dữ liệu xuyên biên giới.

Ở đây chúng ta sẽ tập trung xem xét các nhu cầu an ninh và đề ra các biện pháp an toàn cũng như vận hành các cơ chế để đạt được các mục tiêu đó.

Nhu cầu an toàn thông tin:

- An toàn thông tin đã thay đổi rất nhiều trong thời gian gần đây. Trước kia hầu như chỉ có nhu cầu bảo mật thông tin, nay đòi hỏi thêm nhiều yêu cầu mới như an ninh máy chủ và trên mạng.
- Các phương pháp truyền thống được cung cấp bởi các cơ chế hành chính và phương tiện vật lý như nơi lưu trữ bảo vệ các tài liệu quan trọng và cung cấp giấy phép được quyền sử dụng các tài liệu mật đó.

- Máy tính đòi hỏi các phương pháp tự động để bảo vệ các tệp và các thông tin lưu trữ. Nhu cầu bảo mật rất lớn và rất đa dạng, có mặt khắp mọi nơi, mọi lúc. Do đó không thể không đề ra các qui trình tự động hỗ trợ bảo đảm an toàn thông tin.
- Việc sử dụng mạng và truyền thông đòi hỏi phải có các phương tiện bảo vệ dữ liệu khi truyền. Trong đó có cả các phương tiện phần mềm và phần cứng, đòi hỏi có những nghiên cứu mới đáp ứng các bài toán thực tiễn đặt ra.

Các khái niệm:

- An toàn máy tính: tập hợp các công cụ được thiết kế để bảo vệ dữ liệu và chống hacker.
- An toàn mạng: các phương tiện bảo vệ dữ liệu khi truyền chúng.
- An toàn Internet: các phương tiện bảo vệ dữ liệu khi truyền chúng trên tập các mạng liên kết với nhau.

Mục đích của môn học là tập trung vào an toàn Internet gồm các phương tiện để bảo vệ, chống, phát hiện, và hiệu chỉnh các phá hoại an toàn khi truyền và lưu trữ thông tin.

I.1.2 Nguy cơ và hiểm họa đối với hệ thống thông tin

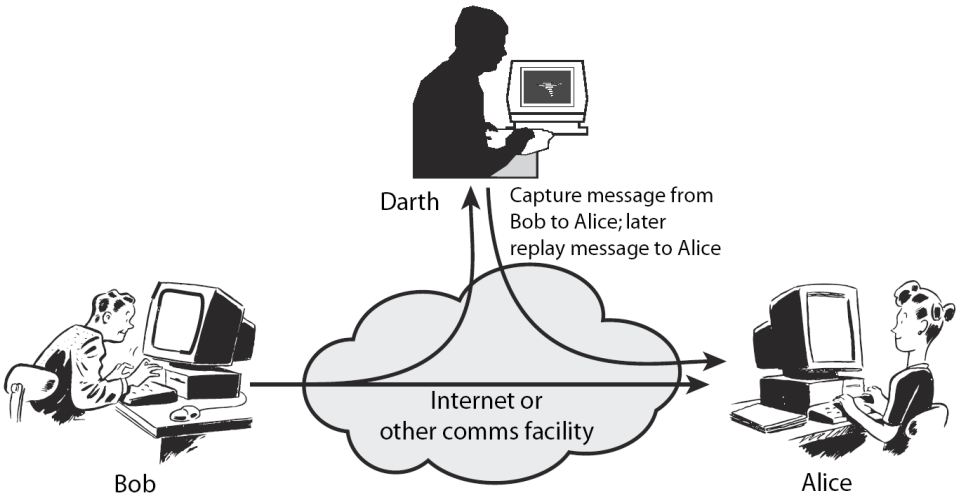
Các hiểm họa đối với hệ thống có thể được phân loại thành hiểm họa vô tình hay cố ý, chủ động hay thụ động.

- Hiểm họa vô tình: khi người dùng khởi động lại hệ thống ở chế độ đặc quyền, họ có thể tùy ý chỉnh sửa hệ thống. Nhưng sau khi hoàn thành công việc họ không chuyển hệ thống sang chế độ thông thường, vô tình để kẻ xấu lợi dụng.
- Hiểm họa cố ý: như cố tình truy nhập hệ thống trái phép.
- Hiểm họa thụ động: là hiểm họa nhưng chưa hoặc không tác động trực tiếp lên hệ thống, như nghe trộm các gói tin trên đường truyền.
- Hiểm họa chủ động: là việc sửa đổi thông tin, thay đổi tình trạng hoặc hoạt động của hệ thống.

Đối với mỗi hệ thống thông tin mối đe dọa và hậu quả tiềm ẩn là rất lớn, nó có thể xuất phát từ những nguyên nhân như sau:

- Từ phía người sử dụng: xâm nhập bất hợp pháp, ăn cắp tài sản có giá trị
- Trong kiến trúc hệ thống thông tin: tổ chức hệ thống kỹ thuật không có cấu trúc hoặc không đủ mạnh để bảo vệ thông tin.
- Ngay trong chính sách bảo mật an toàn thông tin: không chấp hành các chuẩn an toàn, không xác định rõ các quyền trong vận hành hệ thống.
- Thông tin trong hệ thống máy tính cũng sẽ dễ bị xâm nhập nếu không có công cụ quản lý, kiểm tra và điều khiển hệ thống.
- Nguy cơ nằm ngay trong cấu trúc phần cứng của các thiết bị tin học và trong phần mềm hệ thống và ứng dụng do hãng sản xuất cài sẵn các loại 'rệp' điện tử theo ý đồ định trước, gọi là 'bom điện tử'.
- Nguy hiểm nhất đối với mạng máy tính mở là tin tặc, từ phía bọn tội phạm.

I.1.3 Phân loại tấn công phá hoại an toàn:



Các hệ thống trên mạng có thể là đối tượng của nhiều kiểu tấn công:

- Tấn công giả mạo là một thực thể tấn công giả danh một thực thể khác. Tấn công giả mạo thường được kết hợp với các dạng tấn công khác như tấn công chuyển tiếp và tấn công sửa đổi thông báo.
- Tấn công chuyển tiếp xảy ra khi một thông báo, hoặc một phần thông báo được gửi nhiều lần, gây ra các tác động tiêu cực.
- Tấn công sửa đổi thông báo xảy ra khi nội dung của một thông báo bị sửa đổi nhưng không bị phát hiện.
- Tấn công từ chối dịch vụ xảy ra khi một thực thể không thực hiện chức năng của mình, gây cản trở cho các thực thể khác thực hiện chức năng của chúng.
- Tấn công từ bên trong hệ thống xảy ra khi người dùng hợp pháp cố tình hoặc vô ý can thiệp hệ thống trái phép. Còn tấn công từ bên ngoài là nghe trộm, thu chặn, giả mạo người dùng hợp pháp và vượt quyền hoặc lách qua các cơ chế kiểm soát truy nhập.

- Tấn công bị động. Do thám, theo dõi đường truyền để:
  - nhận được nội dung bản tin hoặc
  - theo dõi luồng truyền tin
- Tấn công chủ động. Thay đổi luồng dữ liệu để:
  - giả mạo một người nào đó.
  - lặp lại bản tin trước
  - thay đổi ban tin khi truyền
  - từ chối dịch vụ.

I.2 Dịch vụ, cơ chế, tấn công.

Nhu cầu thực tiến dẫn đến sự cần thiết có một phương pháp hệ thống xác định các yêu cầu an ninh của tổ chức. Trong đó cần có tiếp cận tổng thể xét cả ba khía cạnh của an toàn thông tin: bảo vệ tấn công, cơ chế an toàn và dịch vụ an toàn.
Sau đây chúng ta xét chúng theo trình tự ngược lại:

I.2.1 Các dịch vụ an toàn.

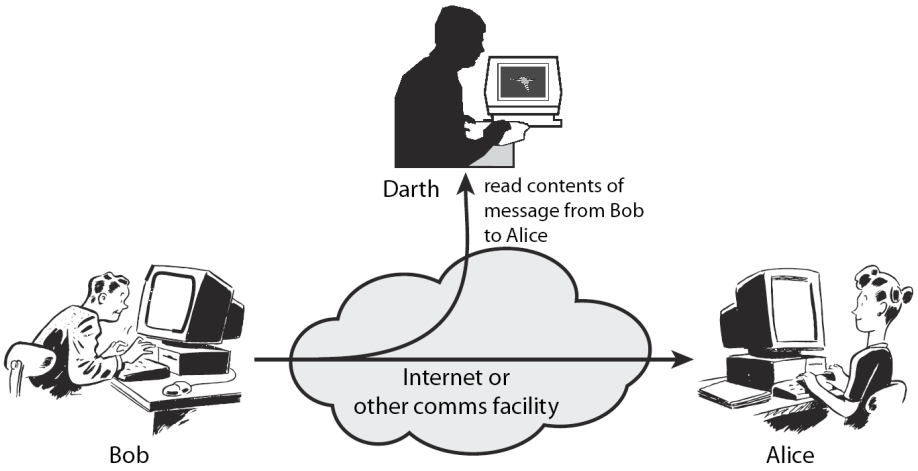
Đây là công cụ đảm bảo an toàn của hệ thống xử lý thông tin và truyền thông tin trong tổ chức. Chúng được thiết lập để chống lại các tấn công phá hoại. Có thể dùng một hay nhiều cơ chế an toàn để cung cấp dịch vụ.
Thông thường người ta cần phải tạo ra các liên kết với các tài liệu vật lý: như có chữ ký, ngày tháng, bảo vệ cần thiết chống khám phá, sửa bậy, phá hoại, được công chứng, chứng kiến, được ghi nhận hoặc có bản quyền.

I.2.2 Các cơ chế an toàn:

Từ các công việc thực tế để chống lại các phá hoại an ninh, người ta đã hệ thống và sắp xếp lại tạo thành các cơ chế an ninh khác nhau. Đây là cơ chế được thiết kế để phát hiện, bảo vệ hoặc khôi phục do tấn công phá hoại.
Không có cơ chế đơn lẻ nào đáp ứng được mọi chức năng yêu cầu của công tác an ninh. Tuy nhiên có một thành phần đặc biệt nằm trong mọi cơ chế an toàn đó là: kỹ thuật mã hoá. Do đó chúng ta sẽ dành một thời lượng nhất định tập trung vào lý thuyết mã.

I.2.3 Tấn công phá hoại an ninh:

Ta xác định rõ thế nào là các hành động tấn công phá hoại an ninh. Đó là mọi hành động chống lại sự an toàn thông tin của các tổ chức.
An toàn thông tin là bàn về bằng cách nào chống lại tấn công vào hệ thống thông tin hoặc phát hiện ra chúng. Trên thực tế có rất nhiều cách và nhiều kiểu tấn công khác nhau. Thường thuật ngữ đe doạ và tấn công được dùng như nhau. Cần tập trung chống một số kiểu tấn công chính: thụ động và chủ động.



I.3 Mô hình an toàn mạng

I.3.1 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 dich 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:

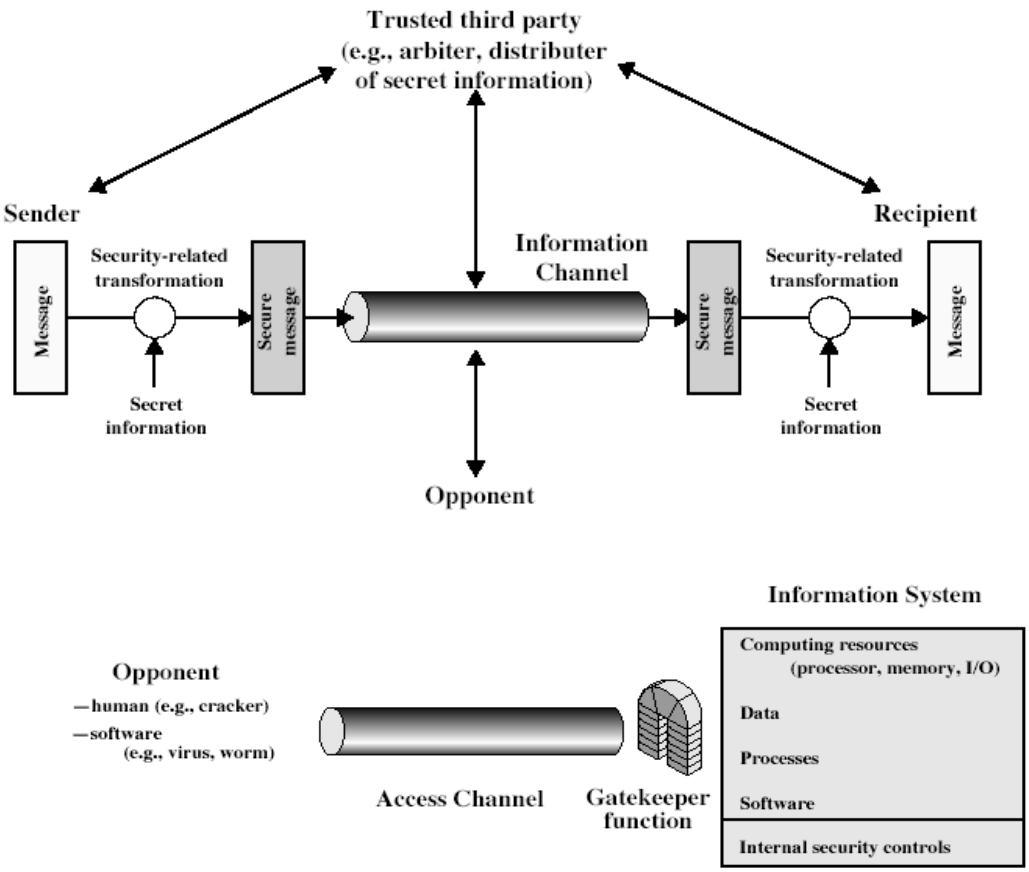
- Cơ chế an toàn chuyên dụng được cài đặt trong một giao thức của một tầng vận chuyển nào đó: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, đệm truyền, kiểm soát định hướng, công chứng.
- Cơ chế an toàn phổ dụng không chỉ rõ được dùng cho giao thức trên tầng nào hoặc dịch 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.

I.3.2 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.

I.4 Bảo mật thông tin trong hệ cơ sở dữ liệu

I.4.1 Giới thiệu chung

Các hệ cơ sở dữ liệu (CSDL) ngày nay như Oracle, SQL/Server, DB2/Informix đều có sẵn các công cụ bảo vệ tiêu chuẩn như hệ thống định danh và kiểm soát truy xuất. Tuy nhiên, các biện pháp bảo vệ này hầu như không có tác dụng trước các tấn công từ bên trong. Để bảo vệ thông tin khỏi mối đe dọa này, người ta đưa ra hai giải pháp.

Giải pháp đơn giản nhất bảo vệ dữ liệu trong CSDL ở mức độ tập tin, chống lại sự truy cập trái phép vào các tập tin CSDL bằng hình thức mã hóa. Tuy nhiên, giải pháp này không cung cấp mức độ bảo mật truy cập đến CSDL ở mức độ bảng, cột và dòng. Một điểm yếu nữa của giải pháp này là bất cứ ai với quyền truy xuất CSDL đều có thể truy