LỜI CẢM ƠN

Em xin chân thành cảm ơn Thầy giáo, Tiến sĩ Phùng Văn Ổn - Trung tâm Công nghệ thông tin Bộ Giao thông vận tải, người đã trực tiếp hướng dẫn tận tình chỉ bảo em trong suốt quá trình làm thực tập tốt nghiệp.

Em xin chân thành cảm ơn tất cả các thầy cô giáo trong Khoa Công nghệ thông tin - Trường ĐHDL Hải Phòng, những người đã nhiệt tình giảng dạy và truyền đạt những kiến thức cần thiết trong suốt thời gian em học tập tại trường, để em hoàn thành tốt đề tài này

Em cũng xin chân thành cảm ơn tất cả các cô chú, các anh chị tại Trung tâm Công nghệ thông tin Bộ Giao thông vận tải, đã giúp đỡ và tạo mọi điều kiện tốt cho em trong thời gian thực tập tại Trung tâm

Tuy có nhiều cố gắng trong quá trình học tập cũng như trong thời gian thực tập nhưng không thể tránh khỏi những thiếu sót, em rất mong được sự góp ý quý báu của tất cả các thầy cô giáo cũng như tất cả các bạn để kết quả của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng, tháng 7 năm 2009

Sinh viên

Nguyễn Thị Phương Thảo

GIỚI THIỆU

Tên đề tài: Nghiên cứu các mô hình bảo mật thông tin, ứng dụng bảo mật hệ thống thông tin của Bộ GTVT.

Mục đích của đề tài:

Tìm hiểu, nghiên cứu các mô hình bảo mật thông tin . Từ đó xây dựng các giải pháp bảo mật thông tin cho các ứng dụng một cách phù hợp .

Để bảo vệ một hệ thống máy tính, trước hết chúng ta cần phải kiểm soát việc truy cập hệ thống. Giải pháp là dùng cách nào đó giới hạn các truy cập của foreign code (foreign code là mã bất kỳ không sinh ra tại máy làm việc nhưng bằng cách này hay cách khác tới được máy và chạy trên đó) tới các dữ liệu và tài nguyên của hệ thống. Chúng ta biết rằng mọi tiến trình đều cần có một môi trường nhất định để thực thi. Đương nhiên một chương trình không bao giờ thực thi sẽ chẳng bao giờ làm hư hại đến hệ thống. Chương trình càng bị giới hạn truy cập tới hệ thống thì hệ thống càng ít nguy cơ rủi ro. Do vậy nguyên tắc chung của chúng ta là kiểm soát nghiêm ngặt việc truy cập của các chương trình tới hệ thống.

Giới thiệu về Bộ GTVT

Ngày 22 tháng 4 năm 2008 Chính phủ đã ban hành Nghị định số 51/2008/NĐ-CP (thay thế Nghị định số 34/2004/NĐ-CP) quy định chức năng, nhiệm vụ, quyền hạn của Bộ Giao thông vận tải.

Chức năng:

Bộ Giao thông vận tải là cơ quan của Chính phủ, thực hiện chức năng quản lý Nhà nước về giao thông vận tải đường bộ, đường sắt, đường sông, hàng hải và hàng không trong phạm vi cả nước; quản lý nhà nước các dịch vụ công và thực hiện đại diện chủ sở hữu phần vốn của nhà nước tại doanh nghiệp có vốn nhà nước thuộc Bộ quản lý theo quy định của pháp luật.

Nhiệm vụ, quyền hạn:

Bộ Giao thông vận tải có trách nhiệm thực hiện nhiệm vụ, quyền hạn quy định tại Nghị định số 178/2007/NĐ-CP ngày 03 tháng 12 năm 2007 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ, cơ quan ngang Bộ và những nhiệm vụ, quyền hạn cụ thể sau đây :

1. Trình Chính phủ dự án luật, dự thảo nghị quyết của Quốc hội, dự án pháp lệnh, dự thảo nghị quyết của Ủy ban Thường vụ Quốc hội; dự thảo nghị quyết, nghị định của Chính phủ theo chương trình, kế hoạch xây dựng pháp luật hàng năm của Bộ đã được phê duyệt và các dự án, đề án theo phân công của Chính phủ, Thủ tướng Chính phủ.

2. Trình Thủ tướng Chính phủ chiến lược, quy hoạch phát triển, kế hoạch dài hạn, năm năm và hàng năm; các chương trình, dự án quốc gia thuộc các lĩnh vực quản lý nhà nước của Bộ; các dự thảo quyết định, chỉ thị của Thủ tướng Chính phủ.

3. Ban hành các quyết định, chỉ thị, thông tư thuộc phạm vi quản lý nhà nước của Bộ; xây dựng để trình cấp có thẩm quyền ban hành hoặc ban hành theo thẩm quyền các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia trong các lĩnh vực quản lý nhà nước của Bộ.

4. Chỉ đạo, hướng dẫn, thanh tra, kiểm tra và chịu trách nhiệm tổ chức thực hiện các văn bản quy phạm pháp luật, chiến lược, quy hoạch, kế hoạch đã được phê duyệt thuộc phạm vi quản lý nhà nước của Bộ; tuyên truyền, phổ biến, giáo dục pháp luật và thông tin về các lĩnh vực quản lý nhà nước của Bộ.

5. Về kết cấu hạ tầng giao thông đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không:

a) Chỉ đạo việc tổ chức thực hiện quy hoạch, kế hoạch phát triển hệ thống kết cấu hạ tầng giao thông đã được Thủ tướng Chính phủ phê duyệt; b) Ban hành quy chuẩn xây dựng và quy định việc quản lý kết cấu hạ tầng giao thông theo thẩm quyền; quy định việc bảo trì, quản lý sử dụng, khai thác kết cấu hạ tầng giao thông (trừ kết cấu hạ tầng giao thông đô thị) trong phạm vi cả nước; chỉ đạo, kiểm tra việc tổ chức bảo trì, bảo đảm tiêu chuẩn, quy chuẩn kỹ thuật mạng lưới công trình giao thông đang khai thác do Bộ chịu trách nhiệm quản lý;

c) Tổ chức thực hiện nhiệm vụ, quyền hạn của cơ quan quyết định đầu tư, chủ đầu tư đối với các dự án đầu tư xây dựng kết cấu hạ tầng giao thông; công bố danh mục dự án gọi vốn đầu tư và hình thức đầu tư kết cấu hạ tầng giao thông theo quy định của pháp luật; d) Trình Chính phủ quy định phạm vi hành lang bảo vệ luồng đường thủy nội địa, hành lang an toàn giao thông đường bộ, hành lang an toàn giao thông đường sắt theo quy định của pháp luật; chỉ đạo, kiểm tra Ủy ban nhân dân các cấp trong việc thực hiện các biện pháp bảo vệ hành lang an toàn giao thông;

đ) Công bố và chỉ đạo tổ chức thực hiện việc đóng, mở cảng hàng không, sân bay và thiết lập đường hàng không sau khi được Thủ tướng Chính phủ cho phép; quyết định việc đóng tạm thời và mở lại cảng hàng không, sân bay; công bố đóng, mở cảng biển, vùng nước cảng biển, luồng hàng hải, cảng, bến thủy nội địa có phương tiện thủy nước ngoài ra vào, tuyến đường thủy nội địa, ga đường sắt, tuyến đường sắt theo quy định của pháp luật;

e) Tổ chức thực hiện việc đăng ký và cấp Giấy chứng nhận đăng ký cảng hàng không, sân bay theo quy định của pháp luật;

g) Trình Chính phủ quy định việc phân loại, đặt tên hoặc số hiệu đường và tiêu chuẩn kỹ thuật của các cấp đường bộ; quyết định phân loại, điều chỉnh hệ thống quốc lộ; hướng dẫn cụ thể việc đặt tên, số hiệu đường bộ.

6. Về phương tiện giao thông, phương tiện, thiết bị xếp dỡ, thi công chuyên dùng trong giao thông vận tải (trừ phương tiện phục vụ vào mục đích quốc phòng, an ninh và tàu cá) và trang bị, thiết bị kỹ thuật chuyên ngành giao thông vận tải:

a) Tổ chức thực hiện việc đăng ký tàu biển, tàu bay theo quy định của Chính phủ; quy định việc đăng ký, cấp biển số phương tiện giao thông đường sắt, đường thủy nội địa và xe máy chuyên dùng tham gia giao thông;

b) Quy định chất lượng an toàn kỹ thuật, bảo vệ môi trường đối với phương tiện giao thông cơ giới;

c) Quy định và hướng dẫn thực hiện tiêu chuẩn, quy chuẩn kỹ thuật, việc kiểm tra chất lượng an toàn kỹ thuật của phương tiện giao thông cơ giới đường bộ, phương tiện giao thông đường sắt, đường thủy nội địa, hàng không, hàng hải, các phương tiện, thiết bị xếp dỡ, thi công chuyên dùng, các công trình, phương tiện, thiết bị chuyên dùng sử dụng trong giao thông vận tải và các mục đích khác theo quy định của pháp luật;

d) Tổ chức cấp Giấy chứng nhận đủ điều kiện bay của tàu bay; cấp Giấy chứng nhận đủ điều kiện bay xuất khẩu đối với tàu bay, động cơ tàu bay, cánh quạt tàu bay khi xuất khẩu; cấp hoặc công nhận Giấy chứng nhận loại đối với tàu bay, động cơ tàu bay, cánh quạt tàu bay khi sản xuất tại Việt Nam hoặc nhập khẩu;

đ) Quy định việc thẩm định thiết kế kỹ thuật trong sản xuất, lắp ráp, sửa chữa, hoán cải phương tiện giao thông, phương tiện, thiết bị xếp dỡ, thi công chuyên dùng và trang bị, thiết bị kỹ thuật chuyên ngành giao thông vận tải;

e) Quy định tiêu chuẩn, quy chuẩn kỹ thuật, điều kiện hoạt động của cơ sở thiết kế, sản xuất, bảo dưỡng hoặc thử nghiệm tàu bay, động cơ tàu bay, cánh quạt tàu bay và trang thiết bị tàu bay tại Việt Nam; cơ sở cung cấp dịch vụ bảo đảm hoạt động bay và cơ sở kiểm định chất lượng an toàn kỹ thuật, bảo vệ môi trường đối với phương tiện giao thông cơ giới đường bộ, đường sắt, đường thủy nội địa, hàng hải, hàng không và các phương tiện, thiết bị, công trình khác theo quy định của pháp luật.

7. Quy định việc đào tạo, huấn luyện, sát hạch, cấp, công nhận, thu hồi giấy phép, bằng, chứng chỉ chuyên môn cho người điều khiển phương tiện giao thông, người vận hành phương tiện, thiết bị chuyên dùng trong giao thông vận tải (trừ người điều khiển phương tiện, thiết bị chuyên dùng phục vụ vào mục đích quốc phòng, an ninh và tàu cá) và cho đối tượng làm việc đặc thù trong lĩnh vực giao thông vận tải.

8. Về vận tải đường bộ, đường sắt, đường thủy nội địa, hàng hải, hàng không dân dụng và vận tải đa phương thức:

a) Hướng dẫn, kiểm tra việc thực hiện điều kiện kinh doanh vận tải, cơ chế, chính sách phát triển vận tải, các dịch vụ hỗ trợ vận tải theo quy định của Chính phủ;

b) Quy định tiêu chuẩn, quy chuẩn kỹ thuật, công nghệ vận hành, khai thác vận tải;

c) Công bố đường bay dân dụng sau khi được Thủ tướng Chính phủ cho phép; công bố các tuyến vận tải đường bộ, đường sắt, đường thủy nội địa và mạng vận tải công cộng theo quy định của pháp luật;

d) Hướng dẫn thực hiện vận tải đa phương thức theo quy định của Chính phủ;

đ) Tổ chức cấp phép hoạt động bay dân dụng; chỉ đạo, kiểm tra việc thực hiện quy chế phối hợp quản lý hoạt động bay dân dụng;

e) Quy định chi tiết việc quản lý hoạt động tại cảng hàng không, sân bay, cảng biển, cảng, bến thủy nội địa, ga đường sắt và tuyến luồng giao thông đường sắt, đường thủy nội địa, hàng hải.

9. Về an toàn giao thông:

a) Chủ trì, phối hợp tổ chức thực hiện các đề án tổng thể về bảo đảm an toàn giao thông trên phạm vi cả nước sau khi được Thủ tướng Chính phủ phê duyệt; hướng dẫn, kiểm tra việc thực hiện các biện pháp bảo đảm an toàn giao thông đường bộ, đường

sắt, đường thủy nội địa, hàng hải, hàng không dân dụng thuộc phạm vi chức năng, nhiệm vụ của Bộ;

b) Phê duyệt chương trình an ninh hàng không dân dụng, phương án điều hành tàu bay bị can thiệp bất hợp pháp, chấp thuận chương trình an ninh hàng không dân dụng của các hãng hàng không nước ngoài; chủ trì thực hiện kiểm tra và cung cấp thông tin an ninh, an toàn hàng không, hàng hải theo quy định của pháp luật;

c) Hướng dẫn các thủ tục điều tra sự cố tai nạn tàu bay theo quy định của Chính phủ; tổ chức thực hiện việc điều tra, xử lý tai nạn hàng hải, hàng không dân dụng theo quy định của pháp luật;

d) Tổ chức thực hiện tìm kiếm - cứu nạn trong giao thông đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không.

10. Về bảo vệ môi trường trong hoạt động giao thông vận tải:

a) Tổ chức thẩm định và phê duyệt báo cáo đánh giá môi trường chiến lược và báo cáo đánh giá tác động môi trường đối với các dự án đầu tư xây dựng kết cấu hạ tầng giao thông và cơ sở sản xuất công nghiệp thuộc thẩm quyền của Bộ theo quy định của pháp luật;

b) Phối hợp với Bộ Tài nguyên và Môi trường, các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ có liên quan và Ủy ban nhân dân cấp tỉnh để chỉ đạo, hướng dẫn, kiểm tra việc thực hiện pháp luật về bảo vệ môi trường và các quy định khác của pháp luật có liên quan đối với xây dựng kết cấu hạ tầng giao thông và hoạt động giao thông vận tải; theo dõi, kiểm tra việc thực hiện các quy định của pháp luật về bảo vệ môi trường trong các lĩnh vực quản lý nhà nước của Bộ;

c) Quy định việc cấp Giấy chứng nhận đạt tiêu chuẩn môi trường đối với phương tiện giao thông cơ giới đường bộ, phương tiện giao thông đường sắt, đường thủy nội địa, hàng hải và hàng không (trừ phương tiện giao thông của quân đội, công an sử dụng vào mục đích quốc phòng, an ninh); chủ trì hướng dẫn kiểm tra, xác nhận tiêu chuẩn môi trường đối với xe ô tô và xe cơ giới khác.

11. Thực hiện hợp tác quốc tế, các Điều ước quốc tế mà Việt Nam đã ký kết hoặc tham gia trong lĩnh vực giao thông vận tải đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không.

12. Chỉ đạo tổ chức thực hiện kế hoạch nghiên cứu khoa học, phát triển và chuyển giao công nghệ trong lĩnh vực giao thông vận tải đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không; chỉ đạo việc xây dựng, triển khai các chương trình, dự án ứng dụng công nghệ thông tin, xây dựng cơ sở dữ liệu, bảo đảm dịch vụ thông tin phục vụ quản lý nhà nước và đáp ứng nhu cầu của tổ chức, cá nhân tham gia hoạt động giao thông vận tải.

13. Về dịch vụ công:

a) Tổ chức thực hiện quy hoạch mạng lưới tổ chức sự nghiệp dịch vụ công trong các ngành, lĩnh vực thuộc phạm vi quản lý nhà nước của Bộ sau khi được cấp có thẩm quyền phê duyệt;

b) Ban hành tiêu chuẩn, quy chuẩn kỹ thuật đối với các hoạt động cung ứng dịch vụ công thuộc ngành giao thông vận tải;

c) Hướng dẫn, hỗ trợ cho các tổ chức thực hiện dịch vụ công theo quy định của pháp luật.

14. Về thực hiện đại diện chủ sở hữu phần vốn của Nhà nước tại doanh nghiệp có vốn nhà nước:

a) Xây dựng đề án sắp xếp, tổ chức lại, chuyển đổi sở hữu doanh nghiệp nhà nước để trình Thủ tướng Chính phủ phê duyệt và chỉ đạo tổ chức thực hiện đề án sau khi được phê duyệt;

b) Trình Thủ tướng Chính phủ bổ nhiệm, bổ nhiệm lại, miễn nhiệm hoặc bổ nhiệm, bổ nhiệm lại, miễn nhiệm theo thẩm quyền các chức danh cán bộ lãnh đạo quản lý, kế toán trưởng của doanh nghiệp nhà nước chưa cổ phần hoá;

c) Trình Thủ tướng Chính phủ phê duyệt hoặc phê duyệt theo thẩm quyền điều lệ tổ chức và hoạt động của doanh nghiệp nhà nước chưa cổ phần hoá. 15. Hướng dẫn, tạo điều kiện cho hội, tổ chức phi Chính phủ tham gia vào hoạt động trong lĩnh vực giao thông vận tải; kiểm tra việc thực hiện các quy định của nhà nước về giao thông vận tải đối với hội, tổ chức phi chính phủ; xử lý hoặc kiến nghị cơ quan nhà nước có thẩm quyền xử lý các vi phạm pháp luật của hội, tổ chức phi Chính phủ theo quy định của pháp luật.

16. Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo, phòng, chống tham nhũng, tiêu cực và xử lý các vi phạm pháp luật về giao thông vận tải đường bộ, đường sắt, đường thủy nội địa, hàng hải và hàng không thuộc thẩm quyền của Bộ.

17. Quyết định và chỉ đạo thực hiện chương trình cải cách hành chính của Bộ theo mục tiêu và nội dung chương trình cải cách hành chính nhà nước đã được Thủ tướng Chính phủ phê duyệt; đề xuất hoặc quyết định theo thẩm quyền việc thực hiện phân cấp quản lý nhà nước về ngành, lĩnh vực. 18. Quản lý về tổ chức bộ máy, biên chế; chỉ đạo thực hiện chế độ tiền lương và các chế độ chính sách đối với cán bộ, công chức, viên chức nhà nước và người lao động thuộc phạm vi quản lý của Bộ; đào tạo, bồi dưỡng, xây dựng đội ngũ cán bộ, công chức, viên chức nhà nước thuộc thẩm quyền; quy định chức danh, tiêu chuẩn cấp bậc kỹ thuật, nghiệp vụ trong các ngành thuộc phạm vi quản lý của Bộ.

19. Quản lý tài chính, tài sản được giao và tổ chức thực hiện quản lý ngân sách được phân bổ theo quy định của pháp luật.

20. Thực hiện các nhiệm vụ khác theo quy định của pháp luật và phân công của Chính phủ, Thủ tướng Chính phủ.

CHƯƠNG 1. VẤN ĐỀ BẢO MẬT HỆ THỐNG THÔNG TIN

1.1. CÁC HIỂM HỌA ĐỐI VỚI MÁY TÍNH VÀ HTTT

Một người muốn truy cập vào hệ thống mạng máy tính có thể vì một lý do này hay một lý do khác. Dưới đây là một số lý do có thể:

- Chỉ để tò mò, giải trí hoặc muốn thể hiện khả năng cá nhân.
- Để xem xét chung chung.
- Để ăn cắp tài nguyên máy tính như thời gian của bộ CPU.
- Để ăn cắp các bí mật thương mại, bí mật quốc gia hoặc các thông tin độc quyền.
- Phát động chiến tranh thông tin trên mạng, làm tê liệt mạng.

Trong mọi trường hợp, bất kể vì lý do gì thì đằng sau vụ tấn công, thông tin mà kẻ phá hoại muốn lấy nhất là password (mật khẩu). Tuy nhiên, mật khẩu đều đã được mã hóa, nhưng điều này không có nghĩa là mật khẩu luôn được an toàn. "Hacker" có thể dùng chương trình Bộ giải mã mật khẩu (Password Cracker) để tìm mật khẩu bằng cách so sánh chúng với các từ trong một từ điển hoặc Brouce Force. Mức độ thành công của chương trình giải mã phụ thuộc vào tài nguyên của CPU, vào chất lượng của từ điển và một vài lý do khác.

Các hình thức tấn công và phá hoại điển hình trên mạng *(LAN và Internet)*

Tấn công theo kiểu từ chối dịch vụ (Denial of Service-DoS)

Hộp thư điện tử thường là mục tiêu tấn công chính của kiểu tấn công này. Tấn công được thực hiện bằng một chương trình gửi thư liên tục đến hộp thư cần phá hoại cho đến khi hộp thư không thể nhận thêm thư được nữa. Hiện nay kiểu tấn công DoS thường nhằm vào các Web Server lớn với mục đích phá hoại dịch vụ cung cấp của Website.

Một biến thể khác của tấn công kiểu DoS là tấn công DoS kiểu phân tán (Distributed Denial of Service - DDoS). Kẻ tấn công sẽ dùng nhiều máy tính bên ngoài đồng loạt tấn công DoS gây ra tắc nghẽn trầm trọng và rất khó truy tìm thủ phạm.

Chặn bắt gói tin (Network Packet Sniffing)

Những chương trình chặn bắt gói tin có thể chặn bất kỳ một gói tin trong mạng và hiển thị nội dung gói tin một cách dễ đọc nhất. Hai đầu của kết nối có thể không biết được gói tin của mình bị xem trộm. Đây là công cụ ưa thích của những người quản trị mạng dùng để kiểm tra mạng. Khi mạng nội bộ được kết nối vào Internet, một

kẻ khả nghi bên ngoài dùng Packet Sniffer có thể dễ dàng chặn gói tin được gửi đến một máy tính nào đó trong mạng và dễ dàng nghe trộm thông tin.

Giả mạo thư IP

Một phương khác được sử dụng là giả mạo địa chỉ IP. Kẻ tấn công sử dụng địa chỉ IP nào đó được tin là hợp lệ, không bị nghi ngờ. Bởi địa chỉ IP là duy nhất nhưng không phải là gắn duy nhất với một máy tính. Khi ai đó muốn đều có thể sử dụng IP mà mình thích mà không cần bất kỳ sự chứng thực nào cả.

Xáo trộn và phát lại thông tin

Các thông tin truyền đi có thể bị chặn lại và thay đổi nội dung rồi mới được gửi đến cho bên nhận (replay attack). Tuy nhiên, việc này sẽ khó thực hiện đối với các mạng truyền quảng bá đến tất cả các máy trạm nhưng dễ dàng thực hiện trong mạng kiểu lưu trữ và chuyển tiếp. Ngoài ra, các thông tin bị chặn lại trên đường truyền còn có thể được lưu lại và gửi vào một thời điểm khác làm cho bên nhận có thể không nhận ra sự thay đổi thông tin. Việc mã hóa thông tin không thể chống lại kiểu tấn công này bởi việc truyền lại các thông tin có thể đúng là thông tin lấy trộm được từ chính tài nguyên của hệ thống thậm chí đối với các kẻ phá hoại không mục đích chúng không cần hiểu hay giải mã được các thông tin mà chúng thực hiện truyền lại.

Một số phương pháp tấn công khác

Hầu hết các phương pháp tấn công trên đều thực hiện do chính người sử dụng hệ thống, chúng lợi dụng quyền của người sử dụng thực hiện chương trình để tiến hành các hoạt động phá hoại

Cùng với các phương thức lấy thông tin bằng truy cập trực tiếp, còn một số phương pháp tinh vi khác khá phổ biến đặc biệt với các hệ thống có đưa ra các dịch vụ truy cập công cộng.

Sử dụng virus máy tính

Là một chương trình gắn vào một chương trình hợp lệ khác và có khả năng lây lan nó vào các môi trường đích mỗi khi chương trình hợp lệ được chạy. Sau khi virus lây nhiễm vào hệ thống nó sẽ thực hiện phá hoại mỗi khi nó muốn, thông thường là phá hoại theo thời gian định trước. Đúng như tên gọi của nó, một trong những hành động của virus đó là lây lan bản thân nó vào tất cả các chương trình mà nó tìm thấy trong môi trường hệ thống. Chúng chuyển từ máy tính này sang máy tính khác mỗi khi chương trình được sao chép bất kể qua mạng hay qua thiết bị lưu trữ vật lý.

Sử dụng chương trình Worm

Là chương trình lợi dụng điều kiện dễ dàng cho phép chạy chương trình từ xa trong hệ phân tán. Các điều kiện này có thể tồn tại một cách tình cờ hoặc có chủ ý. Một số các chương trình Internet Worm đã lợi dụng đặc tính kết hợp cả có chủ ý và tình cờ cho phép chạy chương trình từ xa trong hệ thống BSD UNIX để phá hoại hệ thống.

Sử dụng chương trình Trojan

Những chương trình đưa ra cho người sử dụng hệ thống sử dụng bề ngoài thực hiện một chức năng bình thường nhưng thực chất là thực hiện phá hoại ẩn sau đó.

1.2 AN TOÀN HỆ THỐNG THÔNG TIN

Hệ thống thông tin

Hệ thống thông tin (Information System) là một hệ thống lưu trữ và cung cấp thông tin phục vụ cho hoạt động của con người trong tổ chức. Ta còn có thể hiểu hệ thống thông tin là hệ thống mà mối liên hệ giữa các thành phần của nó cũng như mối liên hệ giữa nó với các hệ thống khác là sự trao đổi thông tin.

Hệ thống thông tin có 4 chức năng chính là: Đưa thông tin vào, lưu trữ, xử lý và đưa ra thông tin.

Các hiểm hoạ mất an toàn đối với hệ thống thông tin

Các hiểm hoạ mất an toàn đối với một hệ thống thông tin có thể được phân loại thành các hiểm hoạ vô tình hay cố ý; các hiểm hoạ chủ động hay thụ động.

***Hiểm họa vô tình* (*unintentional threat*):** Khi người sử dụng tắt nguồn của một hệ thống và khi được khởi động lại, hệ thống ở chế độ single-user (đặc quyền) - người sử dụng có thể làm mọi thứ anh ta muốn đối với hệ thống.

Hiểm họa cố ý* (*intentional threat*):** Có thể xảy ra đối với dữ liệu trên mạng hoặc máy tính cá nhân thông qua các tấn công tinh vi có sử dụng các kiến thức hệ thống đặc biệt. Ví dụ về các hiểm họa cố ý: cố tình truy nhập hoặc sử dụng mạng trái phép (Intentional Unauthorized use of corporate network*).**

***Hiểm hoạ thụ động* (*passive threat*):** Không phải là kết quả của việc sửa đổi bất kỳ thông tin nào có trong hệ thống, hoặc thay đổi hoạt động hoặc tình trạng của hệ thống.

***Hiểm hoạ chủ động (active threat)*:** Là việc sửa đổi thông tin (*Data modification*) hoặc thay đổi tình trạng hoặc hoạt động của một hệ thống.

Mối đe dọa và hậu quả tiềm ẩn đối với thông tin trong giao dịch điện tử là rất lớn. Nguy cơ rủi ro đối với thông tin trong giao dịch điện tử được thể hiện hoặc tiềm ẩn trên nhiều khía cạnh khác nhau như: người sử dụng, kiến trúc hệ thống công nghệ thông tin, chính sách bảo mật thông tin, các công cụ quản lý và kiểm tra, quy trình phản ứng, v.v.

Các yêu cầu cần bảo vệ hệ thống thông tin.

Mục tiêu cuối cùng của quá trình bảo mật thông tin là nhằm bảo vệ ba thuộc tính của thông tin:

- ***Tính bí mật (Confidental):*** Thông tin chỉ được xem bởi những người có thẩm quyền. Lý do cần phải giữ bí mật thông tin vì đó là sản phẩm sở hữu của tổ chức và đôi khi đó là các thông tin của khách hàng của tổ chức. Những thông tin này mặc nhiên phải giữ bí mật hoặc theo những điều khoản giữa tổ chức và khách hàng của tổ chức.

- ***Tính toàn vẹn (Integrity):*** Thông tin phải không bị sai hỏng, suy biến hay thay đổi. Thông tin cần phải xử lý để cách ly khỏi các tai nạn hoặc thay đổi có chủ ý.

- ***Tính sẵn sàng (Availability)***: Thông tin phải luôn được giữ trong trạng thái sẵn sàng cung cấp cho người có thẩm quyền khi họ cần.

Các biện pháp đảm bảo an toàn hệ thống thông tin.

Trong phần này, chúng ta xem xét một số biện pháp bảo mật cho một hệ thống tin học. Cũng cần phảo nhấn mạnh rằng, không có biện pháp nào là hoàn hảo, mỗi biện pháp đều có những mặt hạn chế của nó. Biện pháp nào là hiệu quả, cần được áp dụng phải căn cứ vào từng hệ thống để đưa ra cách thực hiện cụ thể.

Thiết lập quy tắc quản lý

Mỗi tổ chức cần có những quy tắc quản lý của riêng mình về bảo mật hệ thống thông tin trong hệ thống. Có thể chia các quy tắc quản lý thành một số phần:
- Quy tắc quản lý đối với hệ thống máy chủ

- Quy tắc quản lý đối với hệ thống máy trạm

- Quy tắc quản lý đối với việc trao đổi thông tin giữa các bộ phận trong hệ thống, giữa hệ thống máy tính và người sử dụng, giữa các thành phần của hệ thống và các tác nhân bên ngoài.

An toàn thiết bị

- Lựa chọn các thiết bị lưu trữ có độ tin cậy cao để đảm bảo an toàn cho dữ liệu. Phân loại dữ liệu theo các mức độ quan trọng khác nhau để có chiến lược mua sắm thiết bị hoặc xây dựng kế hoạch sao lưu dữ liệu hợp lý.

- Sử dụng các hệ thống cung cấp, phân phối và bảo vệ nguồn điện một cách hợp lý.

- Tuân thủ chế độ bảo trì định kỳ đối với các thiết bị.

Thiết lập biện pháp bảo mật.

Cơ chế bảo mật một hệ thống thể hiện qua quy chế bảo mật trong hệ thống, sự phân cấp quyền hạn, chức năng của người sử dụng trong hệ thống đối với dữ liệu và quy trình kiểm soát công tác quản trị hệ thống. Các biện pháp bảo mật bao gồm:

- Bảo mật vật lý đối với hệ thống. Hình thức bảo mật vật lý khá đa dạng, từ khoá cứng, hệ thống báo động cho đến hạn chế sử dụng thiết bị. Ví dụ như loại bỏ đĩa mềm khỏi các máy trạm thông thường là biện pháp được nhiều cơ quan áp dụng.

- Các biện pháp hành chính như nhận dạng nhân sự khi vào văn phòng, đăng nhập hệ thống hoặc cấm cài đặt phần mềm, hay sử dụng các phần mềm không phù hợp với hệ thống.

+ Mật khẩu là một biện pháp phổ biến và khá hiệu quả. Tuy nhiên mật khẩu không phải là biện pháp an toàn tuyệt đối. Mật khẩu vẫn có thể mất cắp sau một thời gian sử dụng.

+ Bảo mật dữ liệu bằng mật mã tức là biến đổi dữ liệu từ dạng nhiều người dễ dàng đọc được, hiểu được sang dạng khó nhận biết.

+ Xây dựng bức tường lửa, tức là tạo một hệ thống bao gồm phần cứng và phần mềm đặt giữa hệ thống và môi trường bên ngoài như Internet chẳng hạn. Thông thường, tường lửa có chức năng ngăn chặn những thâm nhập trái phép (không nằm trong danh mục được phép truy nhập) hoặc lọc bỏ, cho phép gửi hay không gửi các gói tin

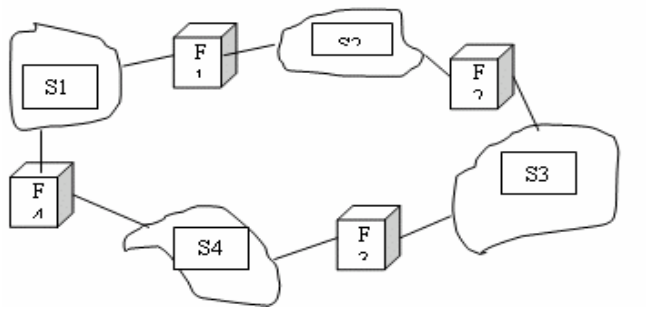
1.3. CÁC CƠ CHẾ BẢO MẬT

Firewall và các cơ chế bảo mật của Firewall.

Thuật ngữ FireWall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ mạng, *FireWall là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống thông tin khác không mong muốn. Nói cách khác FireWall đóng vai trò là một trạm gác ở cổng vào của mạng. FireWall là một giải pháp rất hiệu quả trong việc bảo vệ máy tính khi tham gia*

vào mạng. Nó được coi như là bức tường lửa bảo vệ máy tính của người dùng trước sự tấn công của các hình thức tấn công trên mạng.

Trong một số trường hợp, Firewall có thể được thiết lập ở trong cùng một mạng nội bộ và cô lập các miền an toàn. Ví dụ như mô hình dưới đây thể hiện một mạng cục bộ sử dụng Firewall để ngăn cách phòng máy và hệ thống mạng ở tầng dưới.



Hình 2.1: Mạng cục bộ sử dụng Fire Wall

Chức năng và cấu trúc của FireWall

Chức năng: FireWall là cổng chắn giữa mạng nội bộ với thế giới bên ngoài (Internet), mục đích là tạo nên một lớp vở bọc bao quanh mạng để bảo vệ các máy bên trong mạng, tránh các đe dọa từ bên ngoài. Cơ chế làm việc của tường lửa là dựa trên việc kiểm tra các gói dữ liệu IP lưu truyền giữa máy chủ và trạm làm việc.

FireWall quyết định những dịch vụ nào từ bên trong được phép truy cập từ bên ngoài, những người nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong, và cả những dịch vụ nào bên ngoài được phép truy cập bởi những người bên trong.

Cấu trúc: FireWall bao gồm:

- Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.
- Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

Các thành phần của FireWall

Một FireWall bao gồm một hay nhiều thành phần sau:

- Bộ lọc packet (packet- filtering router).

- Cổng ứng dụng (Application-level gateway hay proxy server).
- Cổng mạch (Circute level gateway).

Nhiệm vụ của FireWall

Nhiệm vụ cơ bản của FireWall là bảo vệ những đối tượng sau:

Dữ liệu: Dữ liệu cần được bảo vệ do những yêu cầu sau:

- *Tính bảo mật (confidentiality):* dữ liệu truyền đi hoặc lưu giữ chỉ được bộc lộ cho những người có đủ thẩm quyền.

- *Tính toàn vẹn (data integrity):* Khả năng phát hiện bất cứ sự thay đổi nào của dữ liệu, điều này đòi hỏi có thể xác nhận được người tạo ra dữ liệu.

- *Tính kịp thời (availability):* Các dịch vụ phải luôn sẵn sàng và hoạt động chính xác.

***Tài nguyên hệ thống*:** Chúng ta phải tốn rất nhiều thời gian và tiền bạc cho tài nguyên và ta có quyền quyết định chúng phải được sử dụng như thế nào. Tài nguyên máy tính không phải là tài nguyên thiên nhiên, nó có giới hạn và không được lãng phí hay phá hủy nếu không được sử dụng.

FireWall chống lại những sự tấn công từ bên ngoài:

- Tấn công trực tiếp:

Cách thứ nhất là dùng phương pháp dò mật khẩu trực tiếp. Thông qua các chương trình dò tìm mật khẩu với một số thông tin về người sử dụng như: ngày sinh, tuổi, địa chỉ v.v…và kết hợp với thư viện do người dùng tạo ra, kẻ tấn công có thể dò được mật khẩu của bạn. Trong một số trường hợp, khả năng thành công có thể lên tới 30%.

Cách thứ hai là sử dụng các lỗ hổng bảo mật do lỗi của các chương trình ứng dụng và bản thân hệ điều hành. Đây là phương pháp đã được sử dụng từ những vụ tấn công đầu tiên và vẫn tiếp tục được sử dụng để chiếm quyền truy cập (có được quyền của người quản trị hệ thống).

- Nghe trộm:

Có một kiểu tấn công cho phép kẻ tấn công lấy được thông tin mà không cần sử dụng máy tính một cách trực tiếp. Phần lớn các kẻ ăn cắp thông tin đều cố gắng truy cập vào hệ thống máy tính bằng cách dò tên người dùng và mật khẩu. Cách dễ nhất để lấy thông tin là đặt máy nghe trộm trên mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy cập vào hệ thống thông qua các chương trình cho phép đưa cạc giao tiếp mạng (Network Interface Card-NIC) vào chế độ nhận

toàn bộ thông tin lưu truyền trên mạng hoặc cài các con rệp (Trojan) vào mạng như là một cổng cung cấp thông tin ra các mạng hoặc thùng thư điện tử bên ngoài.

- Giả mạo địa chỉ IP:

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (source-touting). Với kiểu tấn công này, kẻ tấn công gửi các gói IP tới mạng bên trong một địa chỉ IP giả mạo, đồng thời chỉ rõ đường dẫn mà các gói tin IP phải được gửi đi.

- Vô hiệu hóa các chức năng của hệ thống (deny service):

Đây là kiểu tấn công nhằm làm tê liệt toàn bộ hệ thống không cho nó thực hiện các chức năng mà nó được thiết kế. Kiểu tấn công này không thể ngăn chặn được do những phương tiện tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

- Lỗi người quản trị hệ thống

- Yếu tố con người với những tính cách chủ quan và không hiểu rõ tầm quan trọng của việc bảo mật hệ thống nên dễ dàng để lộ các thông tin quan trọng cho hacker.

Ngày nay, trình độ của các hacker ngày càng giỏi hơn, trong khi đó các hệ thống mạng vẫn còn chậm chạp trong việc xử lý các lỗ hổng của mình. Điều này đòi hỏi người quản trị mạng phải có kiến thức tốt về bảo mật mạng để có thể giữ vững an toàn cho thông tin của hệ thống. Đối với người dùng cá nhân, họ không thể biết hết các thủ thuật để tự xây dựng cho mình một Firewall, nhưng cũng nên hiểu rõ tầm quan trọng của bảo mật thông tin cho mỗi cá nhân, qua đó tự tìm hiểu để biết một số cách phòng tránh những sự tấn công đơn giản của các hacker. Vấn đề là ý thức, khi đã có ý thức để phòng tránh thì khả năng an toàn sẽ cao hơn.

Các nghi thức để xác thực người dùng

Xác thực (Authentication)– Xác thực là quá trình xác nhận tính hợp lệ đối với định danh của một người dùng. Khi một người dùng trình diện định danh của mình, quyền truy nhập và định danh của user đó phải được xác thực. Xác thực đảm bảo một mức độ tin cậy bằng ba nhân tố bao gồm:

1. Những gì bạn biết – Mật khẩu là cách được sử dụng thường xuyên nhất. Tuy nhiên, từ một cụm từ bí mật và số PIN cũng được sử dụng. Chúng được biết dưới tên gọi là xác thực một nhân tố hay xác thực đơn.

2. *Những gì bạn có* - Nhân tố xác thực này sử dụng những gì bạn có, chẳng hạn như một tấm thẻ nhận dạng, smartcard ... Mỗi vật đòi hỏi user phải sở hữu một vật gì

đó để làm vật xác nhận. Đây là một cách xác thực tin cậy hơn đòi hỏi hai nhân tố chẳng hạn như những gì bạn biết với những gì bạn có để nhận thực. Kiểu xác thực này được biết dưới tên gọi xác thực hai nhân tố hoặc xác thực nhiều mức.

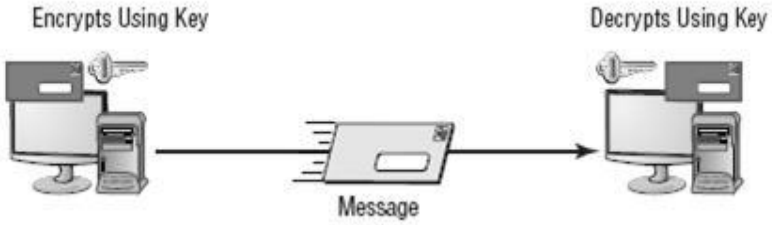
3. *Những gì bạn đại diện cho* - Nhân tố xác thực tốt nhất là những gì mà bạn đại diện cho. Đây là các đặc điểm riêng biệt của cơ thể chẳng hạn như dấu tay, võng mạc, hay ADN. Việc đo lường các nhân tố này gọi là sinh trắc học. Quá trình xác thực tốt nhất này đòi hỏi ba nhân tố. Các phương tiện máy móc hoặc ứng dụng có độ bảo mật cao sẽ dùng ba nhân tố để xác thực một user.

Định danh (Identification) – định danh là số nhận dạng duy nhất. Đó là những gì mà một user sử dụng để phân biệt nó với các đối tượng khác. Một user dùng định danh để chỉ ra anh/chị ta là ai. Định danh được tạo ra cho user không được phép chia sẻ với bất kỳ user hay nhóm user nào khác. Người sử dụng dùng định danh để truy cập đến tài nguyên cho phép.

1.4. CÁC KỸ THUẬT MÃ HOÁ

1.4.1 Hệ mật mã khóa đối xứng(symmetric-key cryptography)

Hệ mật mã khóa đối xứng cũng được gọi là hệ mật mã khóa bí mật. Nó sử dụng một khóa duy nhất để mã hóa và giải mã dữ liệu, đồng thời việc giải mã cũng đòi hỏi thời gian như việc lập mã. Nhưng các hệ mã đối xứng yêu cầu phải giữ bí mật hoàn toàn về khóa lập mã.



Một hệ thống mã hoá đối xứng

Dưới đây là các giải pháp mật mã đối xứng hay sử dụng nhất:

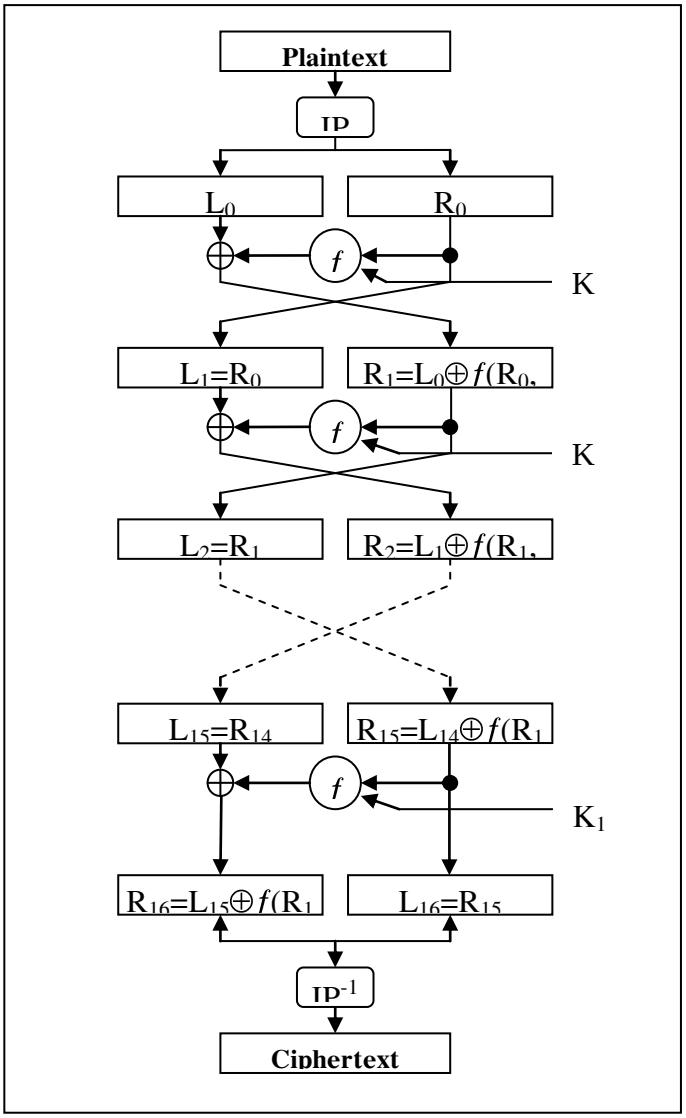
Tên	Block Size	Key Size (bits)
Advanced Encryption Standard (AES) sử dụng thuật toán mã hoá Rijndael	Variable	128, 192, and 256
Triple Data Encryption Standard (3DES)	64	168
Data Encryption Standard (DES)	64	56
International Data Encryption Algorithm (IDEA)	64	128
Blowfish	Variable	1–448
Twofish	128	1-256
Rivest Cipher 5 (RC5)	32, 64, 128	0-2048
Carlisle Adams/Stafford Tavares (CAST-128	64	128

1.4.1.1 Chuẩn mã hoá dữ liệu DES (Data Encryption Standard)

Mô tả thuật toán DES

Thuật toán được thiết kế để lập mã và giải mã một khối dữ liệu nhii phân 64 bits với sự kết hợp của một khóa 64 bits. Quá trình giải mã thực hiện theo mootj sơ đồ như quá trình lập mã, chỉ có khác là trật tự khóa được đảo lại so với quá trình lập mã.

Một khối dữ liệu 64 bits được mã hóa bằng việc cho qua một bảng hoán vị ban đầu (IP – Initial Permutaion) sau đó qua một quá trình tính toán phức tạp có sự tham gia của khóa k được thực hiện, và cuối cùng bản mã nhận được sau khi qua một bảng hoán vị nghịch đảo (IP^{-1} – Inverse ò the Initial Permutation).



Hình 2.4: DES

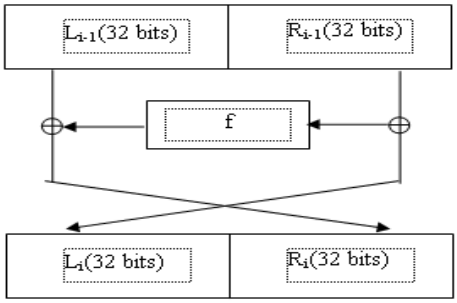
Quá trình mã hóa

64 bits của khối dữ liệu đầu vào được hoán vị bằng bảng IP. Trong đó bits thứ 58 của khối dữ liệu vào là bít đầu tiên, bit thứ 50 của khối dữ liệu vào là bit thứ 2,… và bit cuối cùng của khối dữ liệu sau khi hoán vị là bit thứ 7 của khối dữ liệu vào. Kết quả của phép hoán vị ban đầu sẽ được chia thành 2 nửa L_0R_0 (L_0 = 32 bits là nửa trái, R_0 = 32 bits là nửa phải) sau đó thực hiện 16 lần lặp liên tiếp theo phương pháp:

$L_I = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Và nhận được $L_{16}R_{16}$. Trong đó f được gọi là hàm mật mã. Hàm f có 2 đối là hai khối bits, một là R_{i-1} 32 bits, hai là K_i 48 bits. K_i nhận được từ sơ đồ tạo khóa sẽ được trình bày dưới đây



Kết quả của 16 lần lặp liên tiếp là một khối 64 bits ($R_{16}L_{16}$) được gọi là dữ liệu tienf kết quả (preoutput), khối 64 bits này được cho qua một hoán vị nghịch đảo IP^{-1}. Trong đó bit thứ 40 của khối dữ liệu tiền kết quả là bit đầu tiên, bit thứ 8 của khối dữ liệu tiền kết quả là bit đầu tiên, bit thứ 8 của khối dữ liệu tiền kết quả là bit thứ 2,… và bit cuối cùng sau khi hoán vị là bit thứ 25 của khối dữ liệu tiền kết quả trên. Cuối cùng sau phép hoán vị nghịch đảo ta nhận được bản mã.

Hoán vị khởi đầu

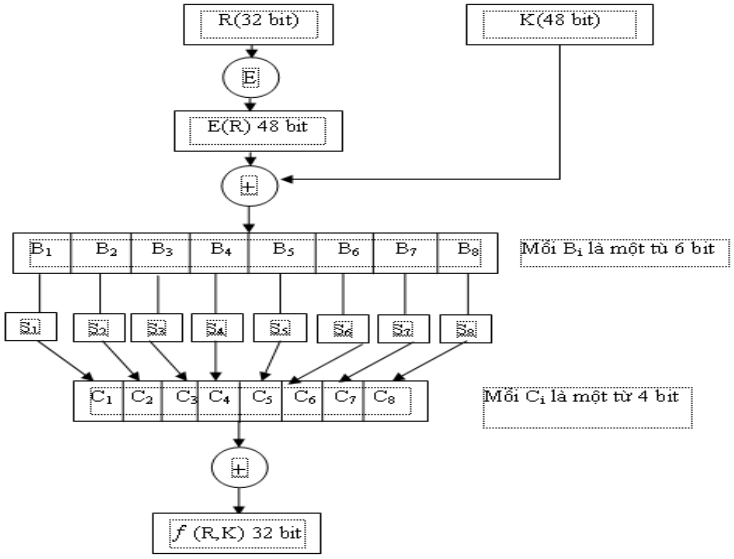
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Hoán vị cuối cùng

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Hàm mật mã f (the cipher function f)

Hàm được tính như sau: $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$



Hàm E là một hoán vị mở rộng. Hàm E thục hiện chức năng mở rộng khối 32 bits thành một khối 48 bits. E(R) có 3 bits đầu lần lượt là các bit thứ 32, 1 và 2 của R,… 2 bits cuối của E(R) là 32 bit và bit 1 của R

Sau đó tính E(R) ⊕ K với K là khóa 48 bits. Kết quả của phép cộng modulo 2 này sẽ được viết thành 8 nhóm, mỗi nhóm 6 bits dạng $B = B_1B_2…..B_8$. Mỗi nhóm B_r 6 bits($1 \le r \le 8$) đó được đưa qua một hộp đen $S_r(S_1S_2……S_8)$ để nhận được $S_r(B_r)$ 4 bits đầu ra. Mỗi hộp S_r là một ma trận 4×16 trong đó mỗi phần tử của S_r là một số nguyên nằm trong khoảng 0→15(có thể biểu diễn tối đa bởi 4 bit nhị phân).

Với mỗi $B_r = b_1b_2b_3b_4b_5b_6$ là các bit của B_r , ta tính $S_r(B_r)$ như sau: b_1b_6 là biểu diễn nhị phân của số hiệu hàng i trong S_r,$b_2b_3b_4b_5$ là biểu diễn nhị phân của số hiệu cột j trong S_r.$C_r = S_r(B_r)$ là phần tử tại hàng I và cột j của S_r.

Ví dụ ta tính $S_1(B)$ với $B = 011011_{(2)}$ thì hàng $i = 01_{(b)} = 1_{(d)}$, cột $j = 1011_{(b)} = 13_{(d)}$. Xác định tại hộp S_1 giá trị tại hàng 1, cột 13 có giá trị là 5 do đó $C = 5_{(d)} = 0101_{(b)}$.

$C = C_1C_2….C_8$ (32 bits) được cho qua một hoán vị P và nhận được kết quả của hàm f:f = P(C).

Hộp E

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	12	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Hộp hoán vị P

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Hộp S thứ 1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Hộp S thứ 2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Hộp S thứ 3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Hộp S thứ 4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Hộp S thứ 5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Hộp S thứ 6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Hộp S thứ 7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Hộp S thứ 8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Giải DES mã

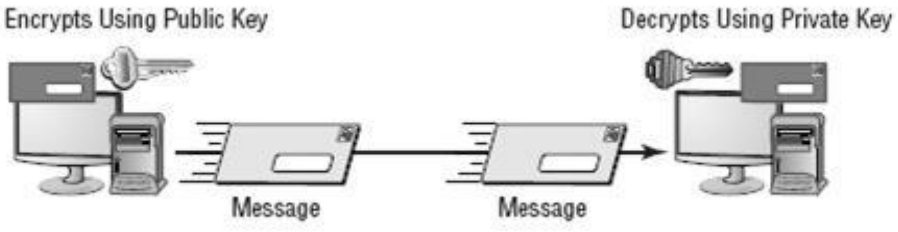
Sau khi thay đổi, hoán vị, XOR, và dịch vòng, chúng ta có thể nghĩ rằng thuật toán giải mã phức tạp, khó hiểu như thuật toán mã hoá và hoàn toàn khác thuật toán mã hoá. Trái lại, sự hoạt động được lựa chọn để đưa ra một đặc tính hữu ích: cùng thuật toán làm việc cho cả mã hoá và giải mã.

Với DES, có thể sử dụng cùng chức năng để giải mã hoặc mã hoá một khối. Chỉ có sự khác nhau đó là các khoá phải được sử dụng theo thứ tự ngược lại. Nghĩa là, nếu các khoá mã hoá cho mỗi vòng là k_1, k_2, k_3 ,... , k_{15}, k_{16} thì các khoá giải là k_{16}, k_{15},... , k_3, k_2, k_1. Giải thuật để tổng hợp khoá cho mỗi vòng cũng tương tự. Có khác là các khoá được dịch phải và số vị trí bit để dịch được lấy theo chiều ngược lại.

1.4.2 Hệ mật mã khóa công khai (public-key cryptography)

Hệ mật mã khóa công khai hay hệ mật mã khóa bất đối xứng, sử dụng một cặp khóa (key) đó là public key và private key. Trong các hệ mật mã khóa công khai, A và B muốn trao đổi thông tin cho nhau thì sẽ thực hiện theo sơ đồ sau. Trong đó B sẽ chọn khóa k=(k', k''). B sẽ gửi khóa lập mã bất kỳ và giữ lại khóa giải mã k''(được gọi là khóa bí mật – private key). A có thể gửi văn bản M cho B bằng cách lập mã theo một hàm $e_{k'}$ nào đó với khóa công khai k' của B trao cho và được bản mã M'=$e_{k'}$(M).

Sau đó gửi M' cho B. Đến lượt B nhận được bản mã M' sẽ sử dụng một hàm giải mã $d_{k''}$ nào đó với khóa bí mật k'' để lấy lại bản gốc $M=d_{k''}(M)$.



Một hệ thống mã hoá sử dụng mật mã khóa công khai

Phương thức mật mã bất đối xứng thường được sử dụng:

- Hệ mật mã Rivest Shamir Adleman (RSA)

- Hệ mật mã Diffie-Hellman

- Hệ mật mã ElGamal dựa trên tính khó giải của bài toán logarit rời rạc

- Hệ mật mã Merkle – hellman (knapsack) hệ mật mã xếp ba lô được xây dựng trên cơ sở của bài toán tập con.

2.4.2.1 Thuật toán mã hoá RSA (Rivest, Shamir, Adleman- các tác giả)

RSA là tên viết tắt từ tên các tác giả của nó Ron Rivest, Adi Shamir, Leonard Adleman - những người đầu tiên giới thiệu thuật toán này năm 1978.

Bài toán RSA: Chi một số nguyên dương n là tích của hai thừa số nguyên tố lẻ p và q. Một số nguyên dương b sao cho gcd(b,(p-1)(q-1))=1 và một số nguyên c. bài toán đặt ra: tìm số nguyên x sao cho $x^b \equiv c(\text{mod } n)$

Thuật toán sinh khóa cho mã khóa Công khai RSA:

1. sinh hai số nguyên tố lớn p và q có giá trị xấp xỉ nhau
2. tính n=p*q, và $\varphi(n) = (p - 1)(q - 1)$
3. chọn một số ngẫu nhiên b, $1 < b < \varphi(n)$ sao cho $\gcd(b, \varphi(n)) = 1$.
4. sử dụng thuật toán Eclide để tính số a, $1< a< \varphi(n)$,sao cho $a*b \equiv 1 \ (\text{mod } \varphi(n))$.
5. khóa công khai là (n,b), khóa bí mật là (a).

thuật toán Mã hóa RSA

(i) Lập mã:

a. Lấy khóa công khai (n,b) theo thuật toán trên

b. Chọn một bản mã x, trong khoảng [1, n - 1]

c. Tính: $y=x^b \bmod n$

d. Nhận được bnả mã y

(ii) Giải mã:

Sử dụng khóa bí mật a để giải mã: $x = y^a \bmod n$

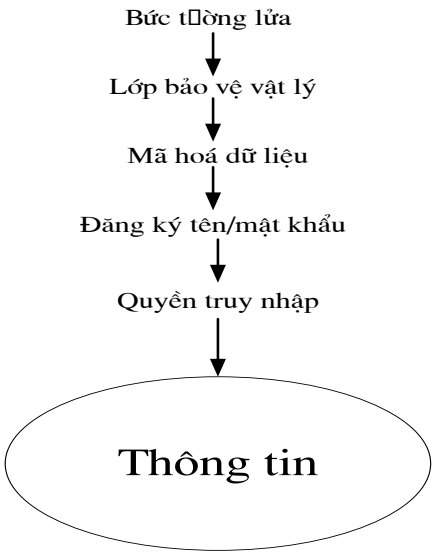
Hệ mã kháo công khai RSA được gọi là an toàn nếu ta chọn số nguyên tố p và q đủ lớn để việc phân tích phần khóa công khai n thành tích hai thừa số nguyên tố là khó có thể thực hiện trong thời gian thực. Tuy nhiên, việc sinh một số nguyên tố được coi là lớn lại là việc rất khó, vấn đề này thường được giải quyết bằng cách sinh ra các số lớn (khoảng 100 chữ số) sau đó tìm cách kiểm tra tính nguyên tố của nó.

Nói chung vấn đè cốt lõi của hệ mã RSA đó là việc chọn lựa số nguyên tố p và q đủ lớn để đảm bảo an toàn cho bản mã. Như đã biết nếu kẻ thám mac mà biết được số nguyên tố thì dễ dàng tính được khóa bí mật (a) từ khóa công khai (b, n) do đó bản mã sẽ bị lộ.

1.4.3. Các chức năng bảo mật khác

Ngoài các phương pháp bảo mật trên, một phương pháp đã và đang được nghiên cứu và ứng dụng rất mạnh mẽ ở nhiều nước trên thế giới đó là phương pháp giấu tin (data hiding). Đây là phương pháp mới và phức tạp, nó đang được xem như một công nghệ chìa khoá cho vấn đề bảo vệ bản quyền, nhận thực thông tin và điều khiển truy cập … ứng dụng trong an toàn và bảo mật thông tin .

Giấu thông tin (Steganography) là một kỹ thuật nhúng thông tin (embeding) vào trong một nguồn đa phương tiện gọi là các phương tiện chứa (host data) mà không gây ra sự nhận biết về sự tồn tại của thông tin giấu (invisible).



Hình 2.13: Các mức bảo mật

Quyền truy nhập (Access Right): Lớp bảo vệ này nhằm kiểm soát việc truy nhập tài nguyên mạng và quyền hạn trên tài nguyên đó. Cụ thể là việc quản lý được tiến hành ở mức truy nhập tệp. Việc xác lập các quyền này được quyết định bởi người quản trị mạng (supervisor).

Đăng ký tên/mật khẩu (login/password): Mỗi người sử dụng muốn vào sử dụng mạng đều phải đăng ký tên/mật khẩu. Nếu người ngoài không biết tên, mật khẩu thì không thể truy nhập vào hệ thống. Nói chung, phương pháp này đơn giản, hiệu quả. Nhưng nếu không cẩn thận để kẻ thâm nhập biết tên, mật khẩu thì có thể gây nguy hiểm. Phương pháp này không mấy hiệu quả với những kẻ quá hiểu biết về hệ thống.

Mã hoá dữ liệu (Data Encryption): Phương pháp này nhằm mục đích biến đổi dữ liệu từ dạng nhận thức được đến dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhập.

Lớp bảo vệ vật lý (Physical Protection): Lớp này nhằm ngăn cản các truy cập vật lý bất hợp pháp vào hệ thống. Thường dùng các biện pháp như cấm tuyệt đối không cho người không có phận sự vào phòng máy, dùng ổ khoá trên máy tính, khoá bàn phím, dùng các trạm không sử dụng ổ đĩa mềm hoặc các biện pháp dùng khoá cứng…

Bức tường lửa (Fire Wall): để bảo vệ an toàn và ngăn chặn từ xa một máy tính hay cả mạng nội bộ (Intranet). Đây là biện pháp tương đối phổ biến để bảo vệ các mạng nội bộ, nó ngăn chặn các thâm nhập trái phép và thậm chí có thể "lọc" bỏ các gói tin mà không muốn gửi đi hoặc nhận vào vì những lý do nào đó.

CHƯƠNG 2. CÁC MÔ HÌNH BẢO MẬT

2.1. GIỚI THIỆU

Để bảo vệ một hệ thống máy tính, trước hết chúng ta cần phải kiểm soát việc truy cập hệ thống. Giải pháp là dùng cách nào đó giới hạn các truy cập của foreign code (foreign code là mã bất kỳ không sinh ra tại máy làm việc nhưng bằng cách này hay cách khác tới được máy và chạy trên đó) tới các dữ liệu và tài nguyên của hệ thống. Chúng ta biết rằng mọi tiến trình đều cần có một môi trường nhất định để thực thi. Đương nhiên một chương trình không bao giờ thực thi sẽ chẳng bao giờ làm hư hại đến hệ thống. Chương trình càng bị giới hạn truy cập tới hệ thống thì hệ thống càng ít nguy cơ rủi ro. Do vậy nguyên tắc chung của chúng ta là kiểm soát nghiêm ngặt việc truy cập của các chương trình tới hệ thống. Có rất nhiều mô hình bảo mật, chẳng hạn như Bell-LaPadula, Take-Grant, Sea View, Biba, Clack-Wilson...

Trước khi nói về các mô hình bảo mật, chúng ta cùng nhìn lại khái niệm về "kiểm soát truy cập" (access control). Đây là một kỹ thuật cơ bản trong bảo vệ thông tin của hầu hết các hệ thống máy tính. Access control có thể được hình dung như là tình huống trong đó một chủ thể chủ động (subject) truy cập một đối tượng bị động (object) với một phép truy cập nào đó. Trong khi một bộ điều khiển tham chiếu (reference monitor) sẽ cho phép hoặc từ chối các yêu cầu truy cập. Mô hình cơ sở của access control được đưa ra bởi Lampson. Trong các hệ thống máy tính, chủ thể là người sử dụng hay các tiến trình. Đối tượng là file, bộ nhớ, các thiết bị ngoại vi, các nút mạng,... Các phép truy cập điển hình là đọc (read), ghi (write), bổ sung (append) và thực thi (execute). Quyền thực hiện một phép truy cập nhất định trên một đối tượng được gọi là quyền truy cập (access right). Các luật bảo mật (security policy) được định nghĩa như một bộ điều phối quyền truy cập cho các chủ thể.

2.2. MÔ HÌNH MA TRẬN TRUY CẬP (ACESS MATRIX MODEL)

Ma trận truy cập là mô hình điều khiển truy nhập cơ bản. Tuy mô hình này được ứng dụng rộng rãi trong các hệ điều hành và cơ sở dữ liệu nhưng nó được phát triển độc lập với các hệ điều hành và các cơ sở dữ liệu.

Trong mô hình này, ứng với mỗi cặp chủ thể - đối tượng có một quyền truy cập nhất định. Quyền truy cập này có thể cho phép hoặc không cho phép sử dụng đối tượng. Hơn nữa, trong trường hợp cho phép thì nó qui định một độ rõ ràng.

Cơ chế hoạt động của ma trận truy cập:

Ma trận truy cập hoạt động theo cơ chế danh sách điều khiển truy cập.

Danh sách điều khiển truy cập (access control list) là danh sách các chủ thể và quyền truy cập tương ứng tới các đối tượng. Danh sách điều khiển truy cập dùng để bảo vệ các đối tượng.

Tồn tại một chủ thể đăc biệt được gọi là supervison. Supervison có thể gán hoặc rút bỏ quyền truy cập của mọi người trong hệ thống. Quyền truy cập có thể là đọc (read), ghi (write), thực hiện (executive), xoá (delete), cập nhật (update)

Mô hình ma trận truy cập được định nghĩa bằng thuật ngữ trạng thái và chuyển đổi trạng thái.

Trạng thái của hệ thống được xác định bởi bộ ba (S,O,A) trong đó:

S: Tập các chủ thể. Tập S là hữu hạn

O: Tập các đối tượng. Tập O là hữu hạn

A: Ma trận truy nhập.

Mỗi phần tử của ma trận A[Si,*Oj*] là danh sách các quyền truy cập của chủ thể Si lên đối tượng Oj, hay là mức độ cho phép truy cập dành cho chủ thể.

Ví dụ: Ma trận truy cập thể hiện trạng thái của một hệ thống gồm:

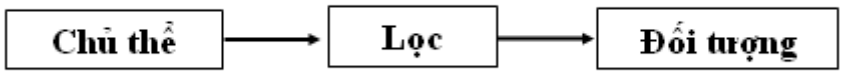
- Hai đoạn bộ nhớ M1 và M2
- Hai file F1 và F2
- Hai tiến trình P1 và P2

Object / Subject	M1	M2	F1	F2
P1	Read Write		Own Read Write	Execute
P2		Read Write		Own Read Execute

Tiến trình P1 có các quyền đọc, ghi đối với đoạn bộ nhớ M1; quyền làm chủ, đọc, ghi với F1; quyền thực hiện F2.

Tiến trình P2 có quyền đọc, ghi đối với đoạn bộ nhớ M2; quyền làm chủ, đọc, thực hiện F2.

Để thực hiện được mô hình này, một bộ kiểm tra đối chiếu được sử dụng. Đó là một cổng giao diện giữa chủ thể và đối tượng. Khi nảy sinh yêu cầu truy cập, nó kiểm tra trên ma trận điều khiển xem yêu cầu này có được thực hiện hay không



Sơ đồ hoạt động của mô hình ma trận truy nhập

Ma trận truy cập thể hiện trạng thái an toàn hiện thời của hệ thống thông tin. Nó bao gồm các hàng là các chủ thể Si, các cột là các đối tượng Oj. Thành phần của ma trận A[Si,Oj] xác định quyền truy cập hiện thời .

Các quyền truy cập thường phụ thuộc vào kiểu đối tượng.

Nếu đối tượng là các file thì quyền truy cập tương ứng là: đọc, ghi, tạo, xoá, sao chép, cập nhật.

Nếu đối tượng là các tiến trình thì quyền truy nhập tương ứng là: chờ đợi, tín hiệu, gửi, nhận, thực hiện.

Ngoài ra còn có các quyền truy cập đặc biệt sau:

Quyền điều khiển: nếu một chủ thể Si tạo ra một chủ thể Sj thì chủ thể Si có quyền điều khiển Sj và có thể xoá bất kì quyền truy cập nào của nó.

Quyền làm chủ: Nếu một chủ thể S tạo ra một đối tượng O thì chủ thể S có quyền làm chủ đối tượng O và có quyền thay đổi quyền truy cập tới đối tượng O của tất cả các chủ thể khác.

Quyền chuyển quyền: Chủ thể S có quyền chuyển quyền đối với một đối tượng O, có thể trao quyền hiện có của mình tới đối tượng O cho một chủ thể khác (quyền được trao phải nhỏ hơn quyền chuyển quyền).

Trạng thái hiện thời của các quyền bảo vệ sẽ thay đổi khi có một quyền mới được trao hay loại bỏ một quyền ra khỏi ma trận truy cập. Tất cả những thay đổi đó sẽ được cập nhật vào ma trận thông qua một bộ kiểm tra ma trận truy cập. Bộ kiểm tra này thực hiện thay đổi nội dung của ma trận truy cập bằng một tập các lệnh bảo vệ; có 8 lệnh trong tập lệnh bảo vệ:

- *Transfer:* Chuyển quyền a cho một chủ thể khác.
- *Grant:* Ban quyền a cho chủ thể khác.
- *Delete:* Xoá quyền a.
- *Read:* Đọc nội dung ma trận truy cập.
- *Create object:* Tạo một đối tượng mới.

- *Delete object:* Xoá một đối tượng đã có.
- *Create subject:* Tạo một chủ thể mới.
- *Delete subject:* Xoá một chủ thể đã có.

Ưu điểm của việc sử dụng ma trận truy cập là supervison có quyền tối cao, điều khiển toàn bộ việc bổ sung hay loại bỏ quyền truy cập của những người sử dụng khác trong hệ thống. Hơn nữa, quyền truy cập của từng chủ thể lên từng đối tượng là rất cụ thể. Mặt khác nó cho phép thay đổi các đối tượng và chủ thể một cách nhanh chóng và dễ dàng. Cơ chế này rất thích hợp với những cơ chế quản lí tập trung.

Tuy nhiên, đối với những hệ thống có số lượng người sử dụng đông đảo, danh sách điều khiển truy cập chở nên phức tạp, cồng kềnh, dẫn đến việc truy cập mất nhiều thời gian, làm giảm hiệu xuất làm việc của hệ thống.

2.3. MÔ HÌNH HRU (HARISON RUZZO – ULLMAN)

Mô hình HRU định rõ hệ thống quyền hạn.

S: là tập các chủ thể

O: là tập các đối tượng

R: là tập các quyền truy cập

Một ma trận truy cập $M = (M_{so})_{s \in S, o \in O}$ với $M_{so} \subset R$

Có 6 hành động nguyên thuỷ:

- nhập r vào trong /từ M_{so}
- tạo/xoá chủ thể S
- tạo/xoá đối tượng O

Sự bảo mật của mô hình HRU:

Các định nghĩa: Một ma trận truy cập M lộ ra quyền r nếu có một lệnh $c : M \to M'$ thêm quyền r vào trong M mà không chứa r trước đó, có nghĩa là $\exists s, o$ sao cho $r \notin M_{s,o}$ và $r \in M'_{s,o}$

Một ma trận truy cập M là an toàn đối với quyền r nếu không có chuỗi lệnh nào có thể biến đổi M thành một trạng thái mà lộ ra r.

Do đó, sự kiểm chứng sự bảo mật có thể chuyển thành sự kiểm chứng đặc tính an toàn.

Định lý:

1. Cho một ma trận truy cập M và một quyền r, sự kiểm chứng độ an toàn của M đối với quyền r là một vấn đề không thể quyết định được.

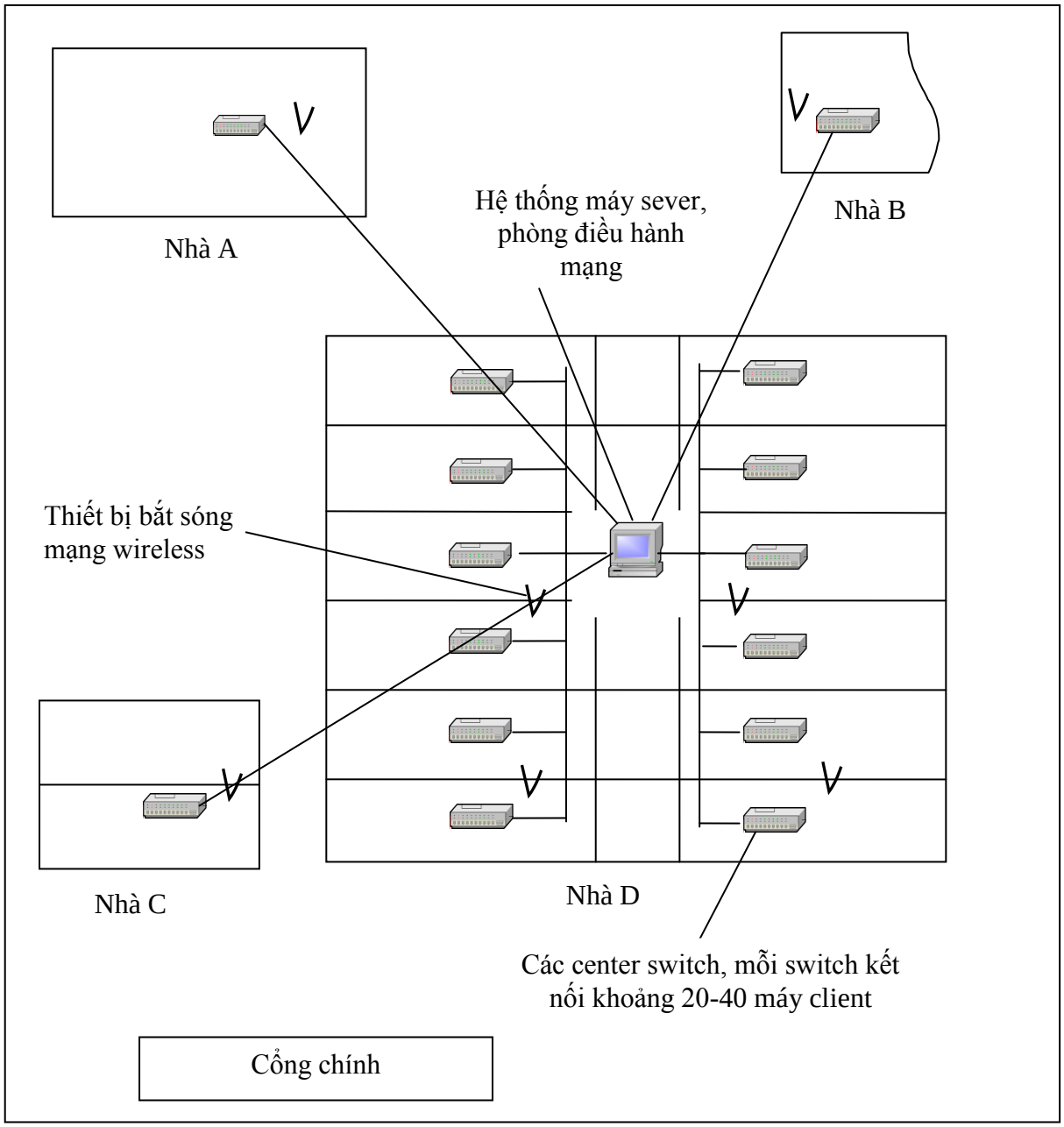
2. Cho một hệ thống quyền hạn toán tử đơn, một ma trận truy cập M và một quyền r, sự kiểm chứng độ an toàn của M đối với r là có thể quyết định được. Còn nếu lệnh do 2 hành động được cho phép chúng tôi lấy không thể quyết định được.

3. Vấn đề an toàn cho các hệ thống quyền hạn là có thể quyết định được nếu số chủ thể được giới hạn.

CHƯƠNG 3. GIỚI THIỆU HỆ THỐNG THÔNG TIN CỦA BỘ GIAO THÔNG VẬN TẢI

3.1 HỆ THỐNG MẠNG

Hệ thống máy chủ, phòng điều hành mạng được đặt tại phòng 421(nhà D)- phòng tích hợp cơ sở dữ liệu và quản trị mạng



Sơ đồ mạng của Bộ Giao thông vận tải

a. Các nhân lực phòng THDL&QTM: 07 người

- Hoàng Mạnh Cường: Trưởng phòng
- Phùng Văn Trọng: Phó trưởng phòng
- Lê Văn Long: Chuyên viên
- Vũ Thuý Hoa: Chuyên viên
- Ngọc Anh Trung: Chuyên viên
- Nguyễn Văn Trường: Chuyên viên
- Hoàng Trung Hiếu: Chuyên viên

b. Thực trạng hạ tầng mạng LAN

Về căn bản các thiết bị mạng đã có sẵn, cụ thể như sau:

Các thiết bị mạng trong phòng 421_trung tâm quản tri mạng

Server: 10 cái

Cisco Switch 2960: 2 cái

Cisco Switch 2950: 1 cái

Cisco Switch HP 2626: 1 cái

PIX 525e: 2 cái

Cisco Router 3745: 2 cái

Cisco Router ASA 5520: 2 cái

Catalyst 2950: 1 cái

Catalyst 3550: 1 cái

Các thiết bị mạng ở nhà D

TT	Tên switch - Vị trí đặt	SL	Số cổng sử dụng/ Tổng số cổng	Ghi chú
1	Cisco2960 24 port (T11) - Tầng 1	01	24/24 + Gi-1,2	VP Bộ
2	Cisco2950 24 port (T12) - Tầng 1	01	23/24	Thanh tra
3	Cisco2950 24 port (T21) - Tầng 2	01	24/24	Vụ KHCN
4	Cisco2950 24 port (T22) - Tầng 2	01	10/24	Vụ HTQT
5	Planet 24 port (T311) - Tầng 3	01	24/24	Vụ TCCB
6	Planet 24 port (T312) - Tầng 3	01	18/24	Vụ TCCB
7	HP 24 port (T32) - Tầng 3	01	23/24	Vụ KHĐT

8	Cisco2950 24 port (T421) - Tầng 4	01	20/24	Vụ PC/KHĐT
9	Cisco2950 24 port (T422) - Tầng 4	01	15/24	Vụ Vận tải
10	Cisco2950 24 port (TIC) - Tầng 6	01	22/24	TT CNTT
11	Switch 16 port (P.401) - Tầng 4	01		Vụ KHĐT

1. Nhận xét ứng dụng CNTT tại Bộ GTVT

Một số ứng dụng đã được triển khai, có ảnh hưởng tích cực và hiệu quả vào công tác quản lý, điều hành; góp phần tích cực đổi mới phong cách làm việc của cán bộ công chức. Cụ thể:

Các ứng dụng điển hình tại Bộ GTVT:

- WEBSITE Bộ GTVT, với thông tin khá phong phú, cập nhật nhanh (3 lần/ngày) phản ánh các hoạt động chỉ đạo, điều hành của Lãnh đạo Bộ và hoạt động của các đơn vị trong ngành. Lượng truy cập tương đối cao, khoảng 5000-6000 lượt mỗi ngày. 9 tháng đầu năm 2008 đã đạt 1.000.000 lượt truy cập.

- Hệ thống thư điện tử của Bộ GTVT với gần 400 địa chỉ thư đang hoạt động hiệu quả.

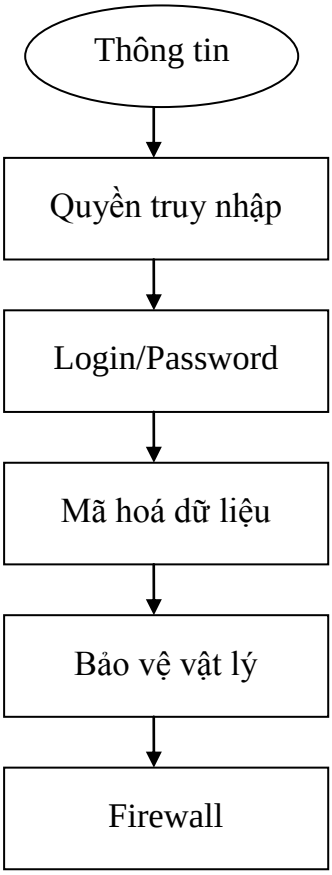
- Phần mềm hỗ trợ công tác quản lý và điều hành như quản lý văn bản đi/đến, văn bản trình ký, lịch làm việc của Lãnh đạo Bộ.

- Các cơ sở dữ liệu: VB QPPL về GTVT, VB điều hành, Tiêu chuẩn công nghệ ngành GTVT được công khai trên Internet.

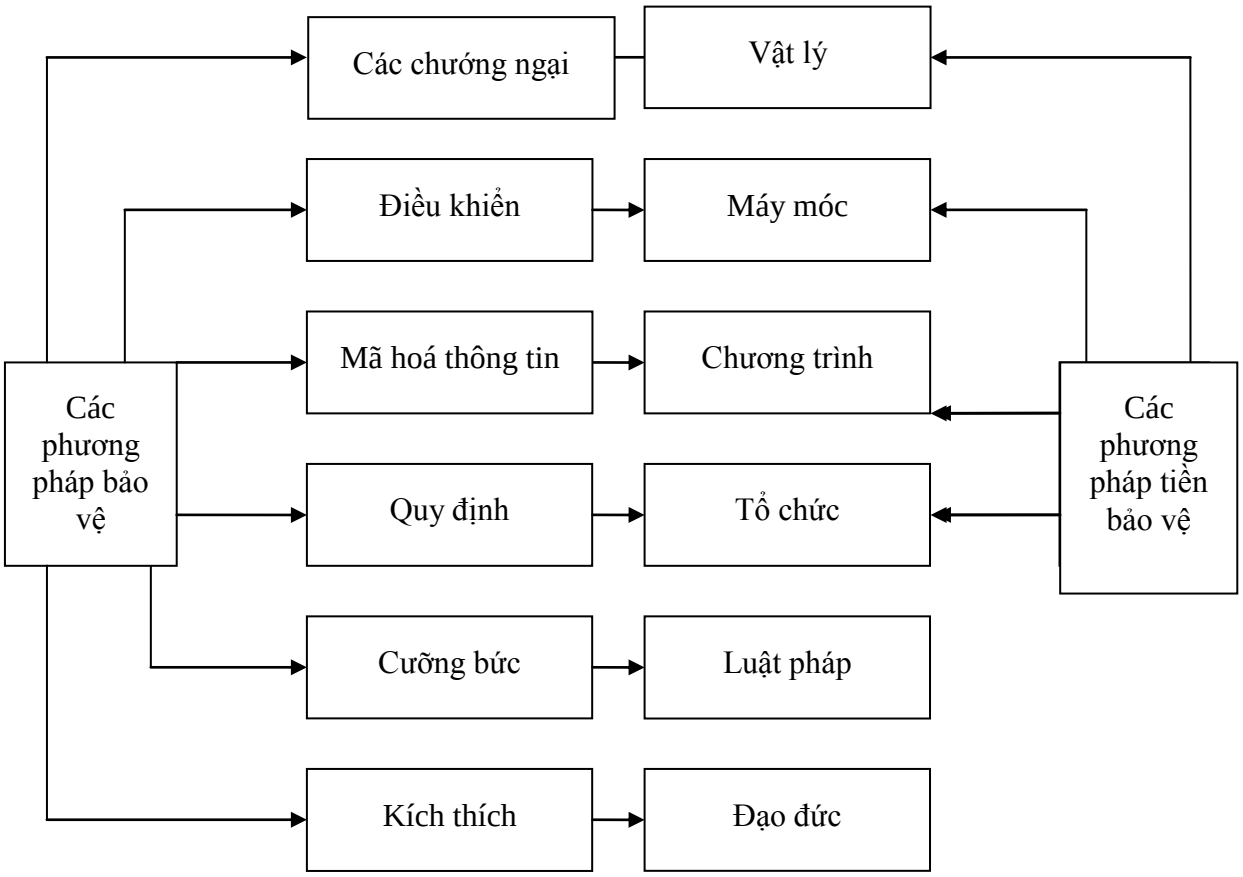
- Các trang thông tin điện tử chuyên ngành như: CCHC, Thanh tra GTVT, KHCN, Thông tin đấu thầu các dự án GTVT.

3.2 CÁC CƠ CHẾ BẢO MẬT ÁP DỤNG TẠI TRUNG TÂM CNTT

3.2.1. Xây dựng các mức bảo vệ thông tin.



3.2.2. Các phương pháp và phương tiện bảo vệ thông tin trên mạng



Cơ chế vật lý và quy định:

Hệ thống mạng của Bộ GTVT được quản lý trực tiếp bởi trung tâm công nghệ thông tin. Các Server lưu trữ dữ liệu được đặt ở phòng riêng, chỉ cho những người có chức năng và thẩm quyền được vào. Có nội quy sử dụng và truy cập mạng một các rõ ràng thông qua các tài khoản. Các quy định đều được phổ biến rộng rãi cho mọi người sử dụng đúng mục đích và an toàn.

3.2.3 Cơ chế an toàn trên hệ điều hành

Cơ chế làm việc chung trên mạng

- Nhiều người đồng thời sử dụng các dịch vụ mạng (Multiuser)
- Nhiều ứng dụng cùng chạy tại một máy trạm (Multitasking).
- Tài nguyên và bộ nhớ được chia sẻ giữa các ứng dụng và người dùng (Sharing).
- Tiêu chuẩn an toàn cho các hệ điều hành

• Dễ dàng đăng nhập an toàn (Secure log-on facility): Chỉ cần một user ID và một password.

- Điều khiển truy nhập tuỳ ý (Discretionary access control): mỗi user có thể quyết định cho phép người khác truy nhập ở mức độ nào đối với các file của anh ta.
- Kiểm soát: hệ điều hành phải phát hiện và ghi lại tất cả các sự kiện liên quan đến tính an toàn của hệ thống.
- Bảo vệ bộ nhớ (Memory protection): bộ nhớ phải có thể được bảo vệ khỏi việc đọc, ghi không được xác thực. Toàn bộ bộ nhớ phải được khởi tạo lại trước khi chúng được tái sử dụng, vì thế nội dung của các bản ghi trước đó sẽ không bị mất.
- Điều khiển truy nhập bắt buộc: hệ điều hành phải duy trì một mức an toàn riêng cho mỗi user và mỗi đối tượng.

Cơ chế an toàn hệ điều hành

- Mọi thông tin và thiết bị trên mạng phải chịu sự quản lý của hệ thống. Mọi người khi truy nhập vào hệ thống và tài nguyên phải được kiểm soát, tránh lạm dụng quyền hạn sử dụng hoặc tìm cách vượt quá quyền hạn cho phép.

- Cơ chế an toàn của hệ điều hành mạng có nhiệm vụ quản lý và phân quyền cho người sử dụng đối với các tài nguyên mạng. Cơ chế quản lý càng cụ thể và chặt chẽ càng làm tăng độ an toàn cho các mạng máy tính.

- Mọi tài nguyên trên mạng được chia sẻ về các miền và các nhóm làm việc hay các thiết bị mạng. Mọi tài nguyên trên mạng được các hệ điều hành mạng phân cấp quản lý chặt chẽ theo vai trò người sử dụng trong miền hay nhóm làm việc. Cơ chế quản lý theo miền là cơ chế quản lý chặt chẽ và tập trung do đó nó có độ an toàn cao.

Cơ chế quản lý của hệ điều hành mạng như sau:

- Mỗi tài nguyên được gán các mức truy nhập như thao tác đối với máy in, các thao tác đọc ghi, xoá hay tổ hợp của chúng đối với tệp, thư mục. Mỗi người sử dụng có một tập các quyền đối với các tài nguyên. Tuỳ theo vai trò của người sử dụng mà tập này lớn hay nhỏ. Người quản trị mạng là người có nhiều quyền hạn nhất.

- Hệ thống không chỉ phân chia quyền hạn mà còn phải kiểm soát quyền sử dụng đúng như đã phân chia, bao gồm việc kiểm soát chặt chẽ tài nguyên và người sử dụng.

- Muốn một hệ điều hành mạng an toàn người ta phải xây dựng chính sách an toàn cho nó. Chính sách an toàn phải chặt chẽ và rất đầy đủ. Sau đó người ta xây dựng các mô hình an toàn dựa trên các chính sách an toàn. Các mô hình này phải phản ánh đúng các chính sách an toàn và dễ thực thi. Cuối cùng là cài đặt mô hình an toàn vào hệ điều hành mạng đã xây dựng.

Các vấn đề cần quan tâm đối với hệ thống an toàn hệ điều hành

- Bộ nhớ (memory): Bộ nhớ phải được phân chia và sử dụng độc lập giữa những người sử dụng và ứng dụng.

- Các thiết bị vào ra (I/O devices): Các thiết bị vào ra phải được sử dụng tách biệt giữa các ứng dụng, người sử dụng như các ổ đĩa chẳng hạn.

- Các thiết bị ngoại vi: Các thiết bị ngoại vi như máy in, máy vẽ,...cần được bảo vệ và phân quyền sử dụng.

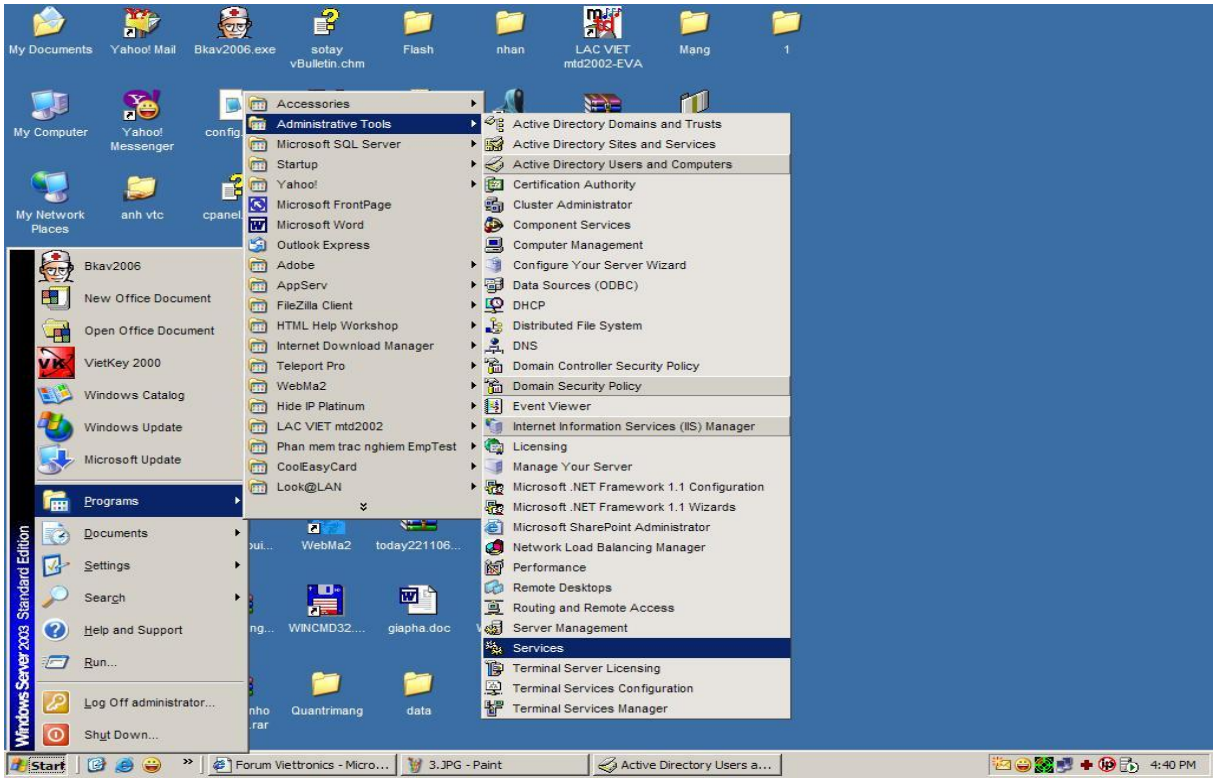
- Các ứng dụng và các chương tình con chia sẻ: cần được bảo vệ và phân cấp sử dụng tốt.

- Số liệu chia sẻ: Cần được bảo vệ và sử dụng đúng quyền hạn giữa những người sử dụng và ứng dụng.

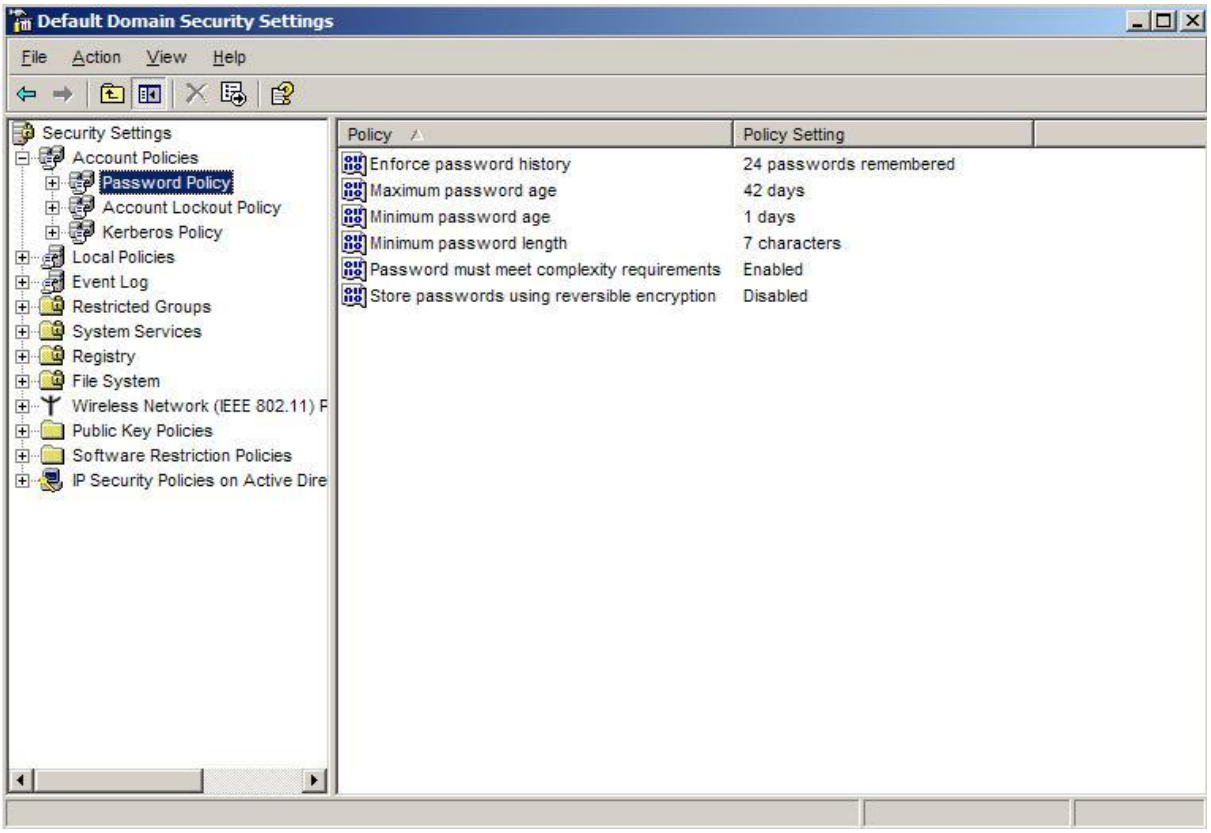
Cài đặt cơ chế an toàn cho hệ thống mạng Window server 2003

- Để cài đặt cơ chế an toàn cho hệ thống, ta thực hiện thiết lập chính sách bảo mật Domain như sau:

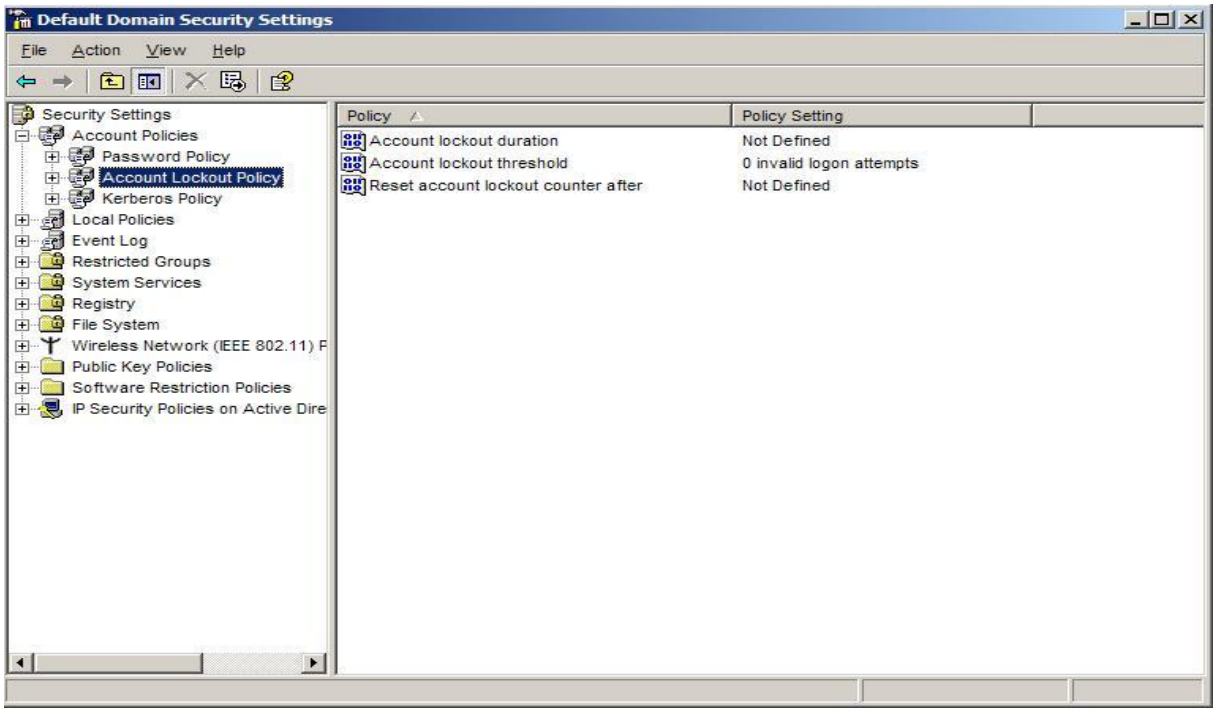
Start – Program – Adminstrator Tools – Domain Security Policy.



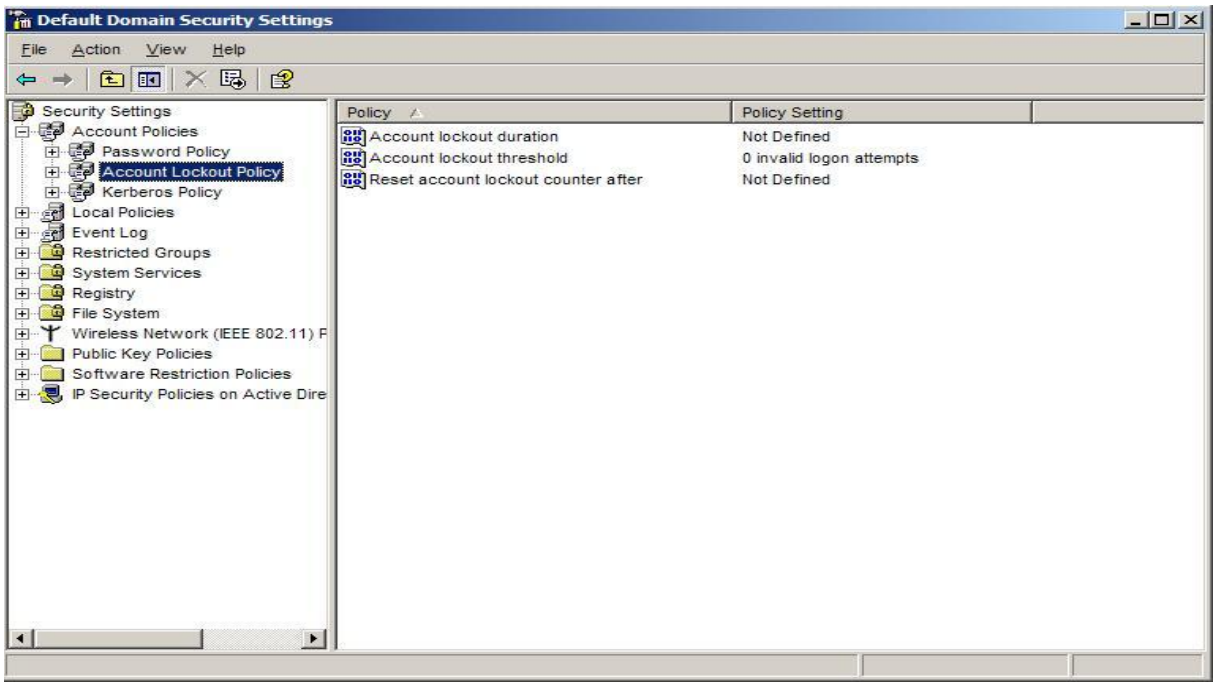
Công cụ quản trị hệ thống



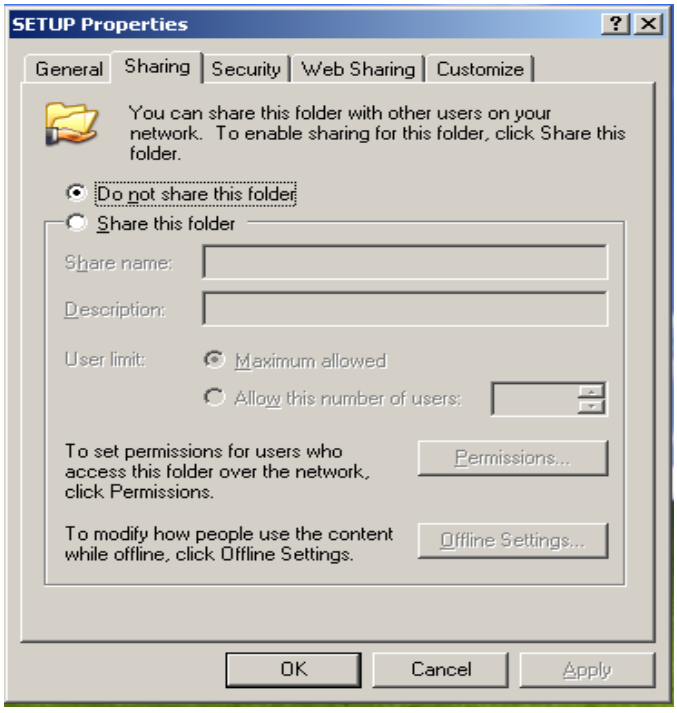
Chính sách về mật khẩu



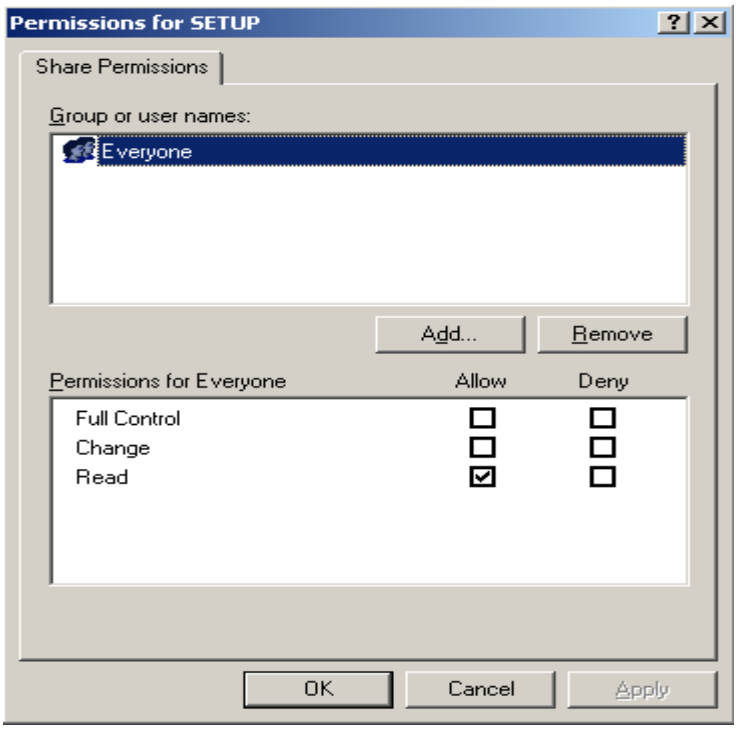
Chính sách khoá khoản mục

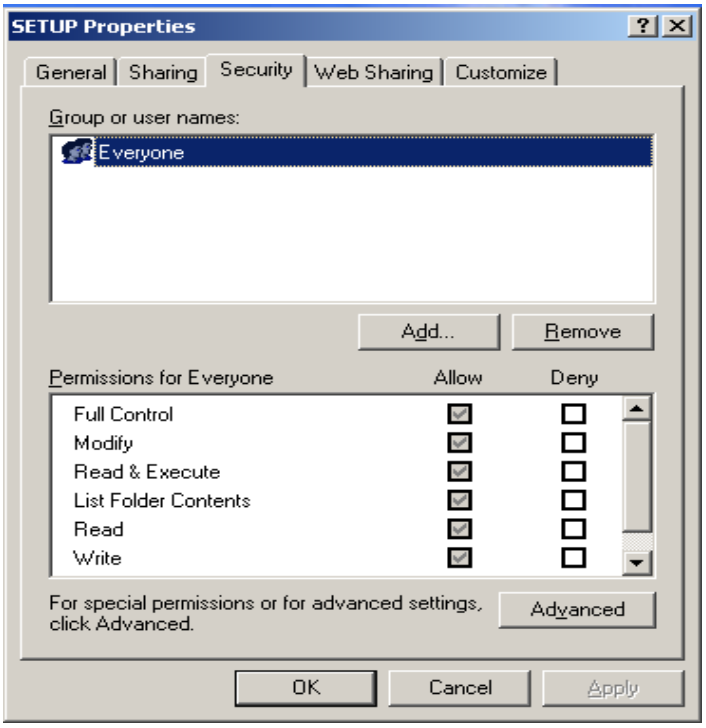


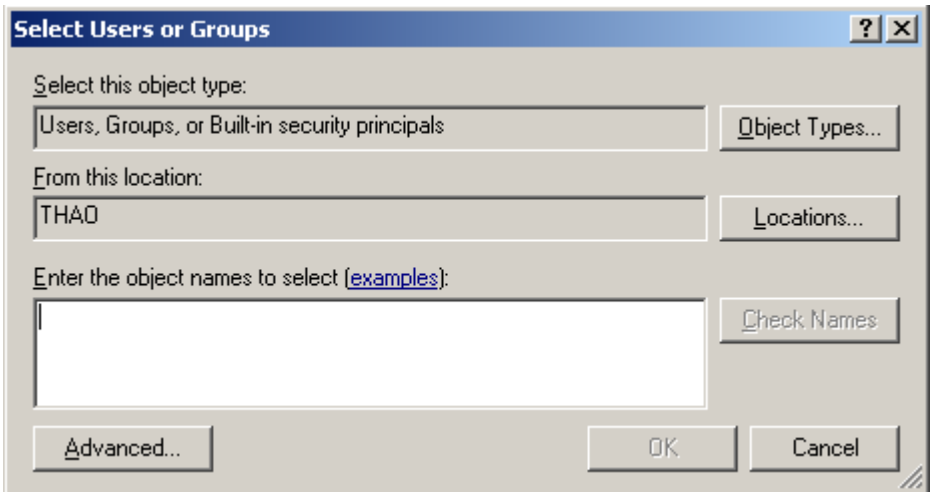
Hình 4.9. Quyền hạn của người dùng

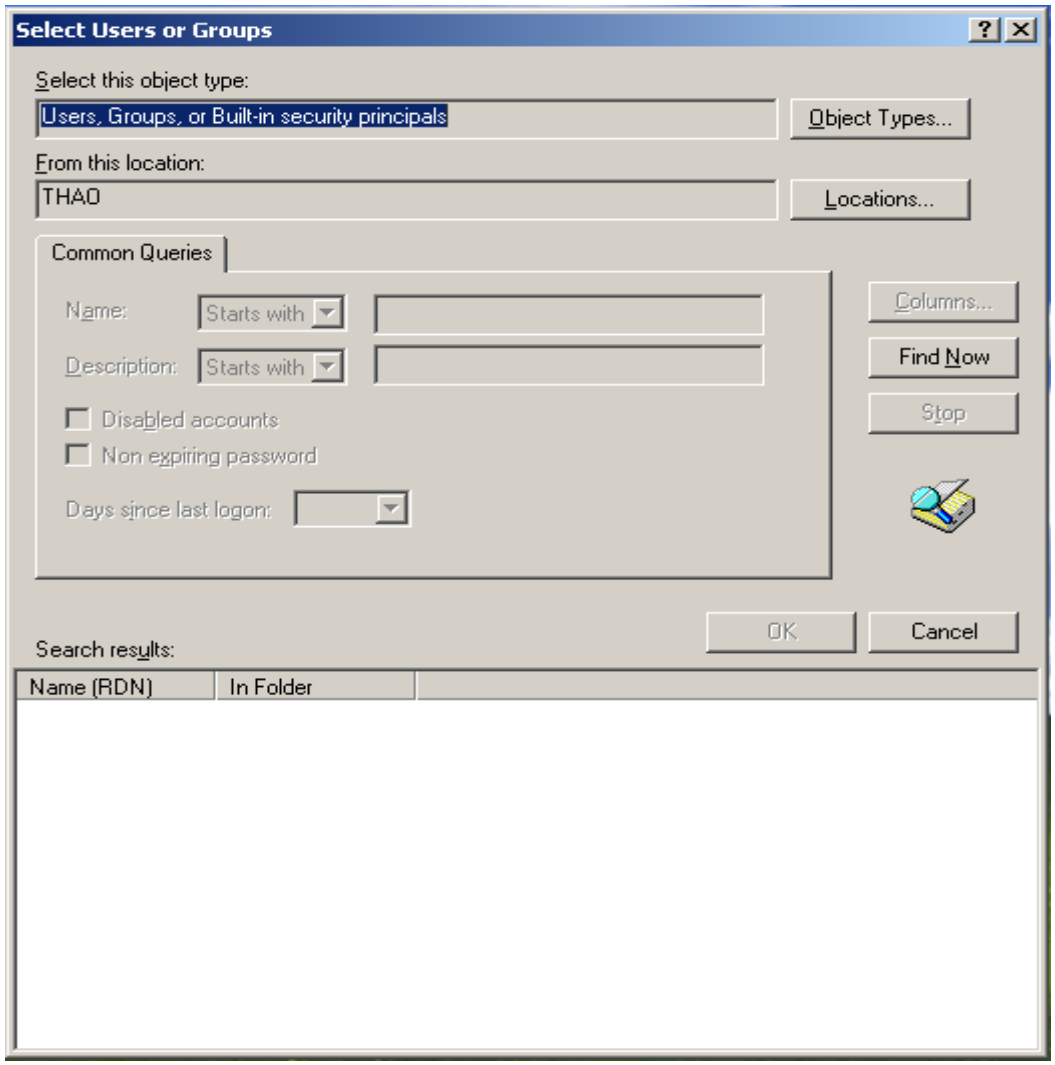


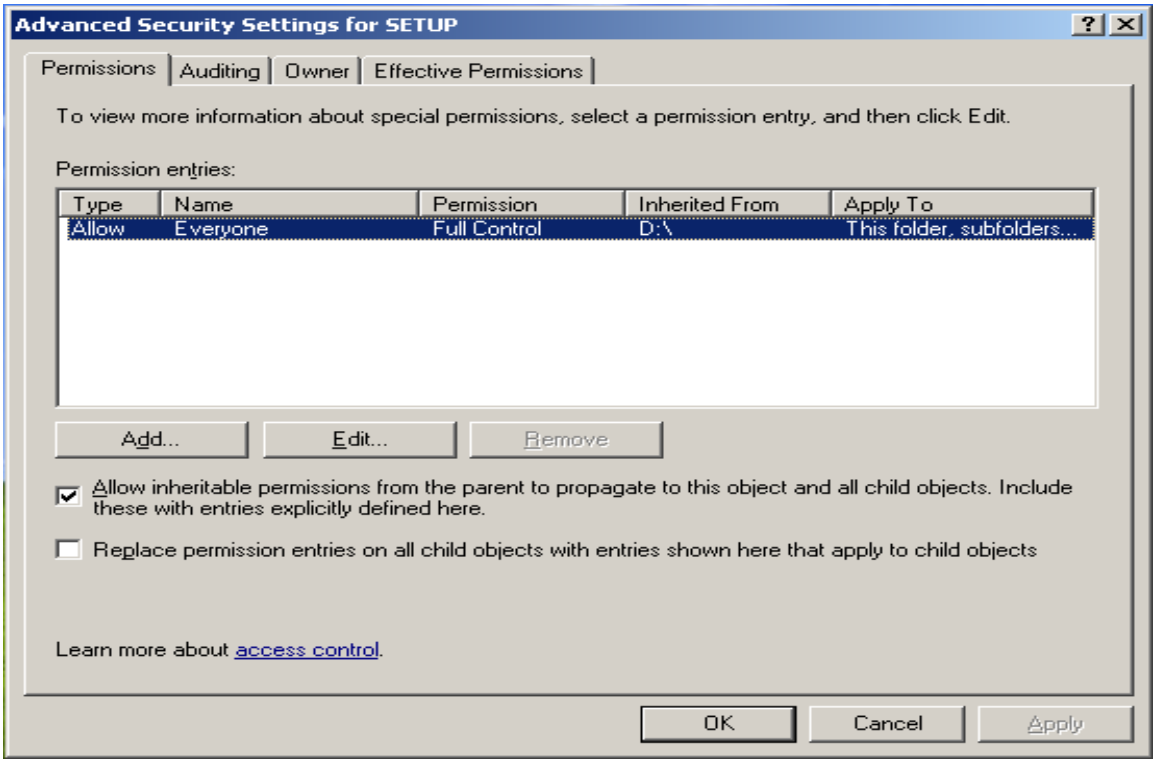
Hình 4.10. Gán quyền truy nhập từ xa

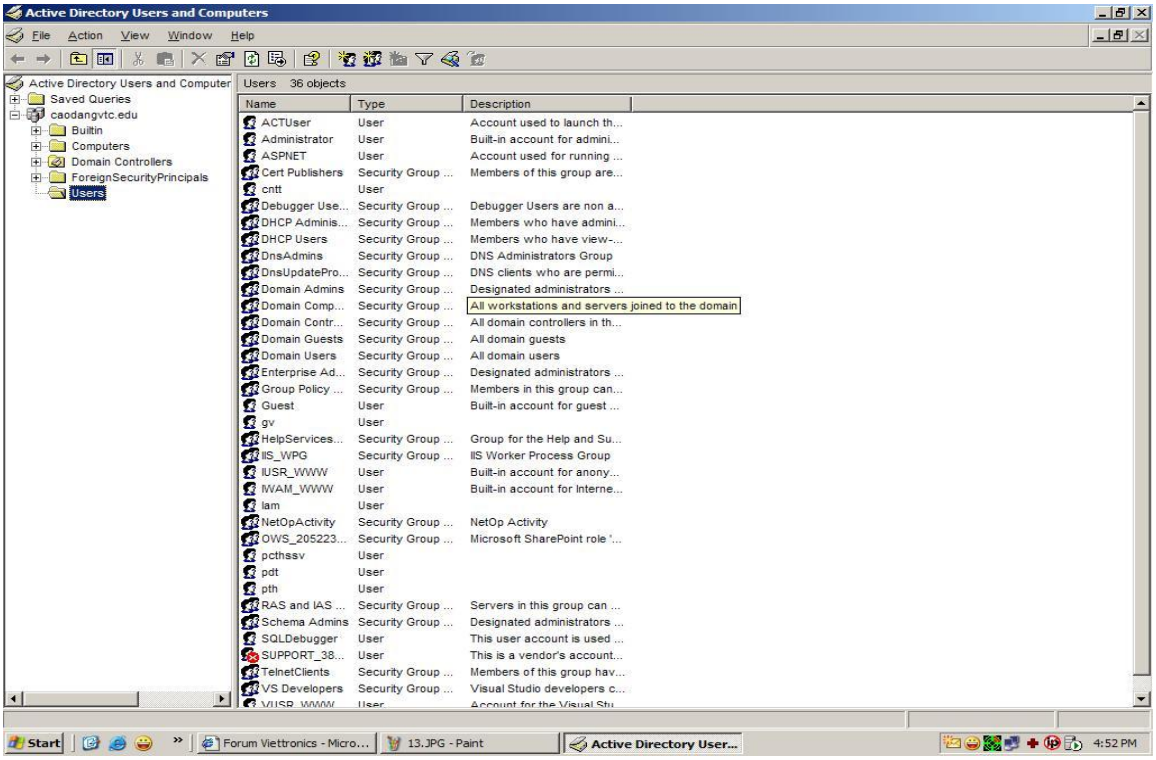

Permissions for SETUP
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

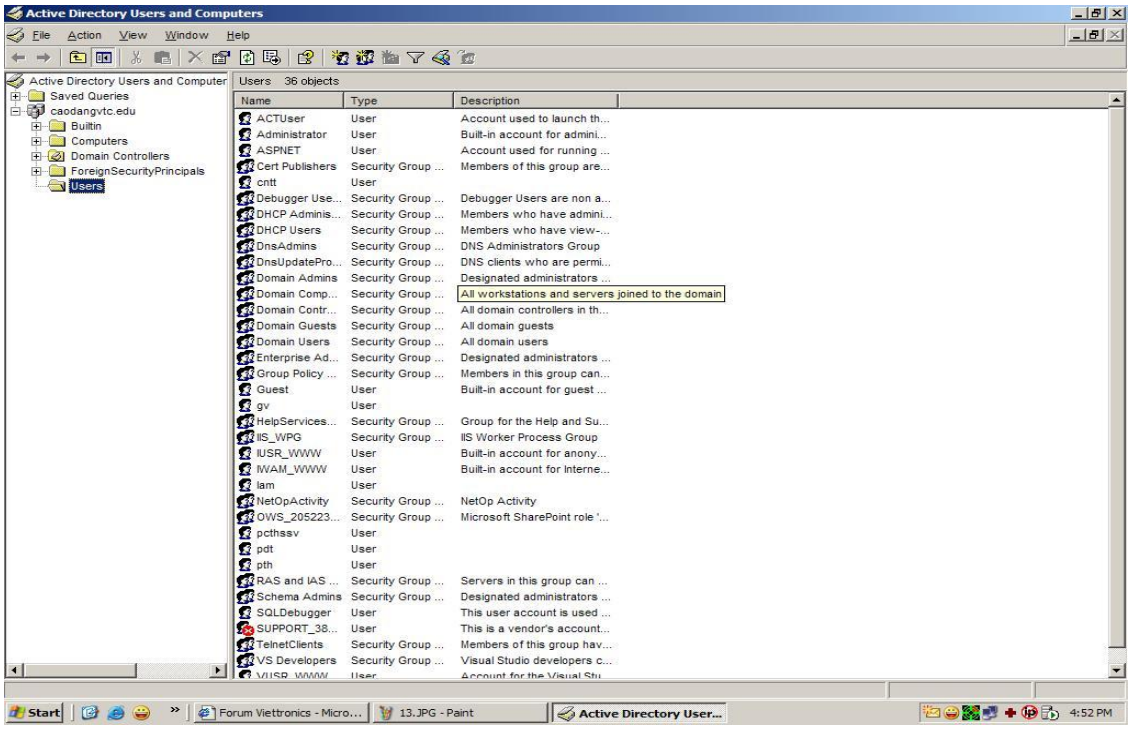

SETUP Properties
General
Sharing
Security
Web Sharing
Customize
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Modify
Read & Execute
List Folder Contents
Read
Write
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply


Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
THAO
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel


Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
THAO
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name (RDN)
In Folder


Advanced Security Settings for SETUP
Permissions
Auditing
Owner
Effective Permissions
To view more information about special permissions, select a permission entry, and then click Edit.
Permission entries:
Type
Name
Permission
Inherited From
Apply To
Allow
Everyone
Full Control
D:\
This folder, subfolders...
Add...
Edit...
Remove
Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.
Replace permission entries on all child objects with entries shown here that apply to child objects
Learn more about access control.
OK
Cancel
Apply


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computer
Saved Queries
caodangvtc.edu
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Users 36 objects
Name
Type
Description
ACTUser
Administrator
ASPNET
Cert Publishers
cntt
Debugger Use...
DHCP Adminis...
DHCP Users
DnsAdmins
DnsUpdatePro...
Domain Admins
Domain Comp...
Domain Contr...
Domain Guests
Domain Users
Enterprise Ad...
Group Policy ...
Guest
gv
HelpServices...
IIS_WPG
IUSR_WWW
IWAM_WWW
lam
NetOpActivity
OWS_205223...
pcthssv
pdt
pth
RAS and IAS ...
Schema Admins
SQLDebugger
SUPPORT_38...
TelnetClients
VS Developers
All workstations and servers joined to the domain
Start
Forum Viettronics - Micro...
13.JPG - Paint
Active Directory User...
4:52 PM



3.2 ĐỀ XUẤT CÁC CƠ CHẾ BẢO MẬT CHO BỘ GTVT

Cài đặt phần mềm Firewall (phần mềm ISA 2006)

Sơ lược về ISA 2006

Như mọi người đã biết nếu ta Publish a Web Server, FTP, DNS Server,… thì khi hacker tấn công vào các Server của chúng ta, các Server sẽ chịu tác động trực tiếp, như thế nội dung Website sẽ bị thay đổi dẫn đến tổ chức, doanh nghiệp có thể bị thiệt hại về mặt nào đó. Vì vậy ta nên cài ISA hay các phần mềm Firewall khác để bảo vệ các Server cũng như Internal network của chúng ta

- Vì sao cài ISA, các Server có thể tránh được các cuộc tấn công trực tiếp.

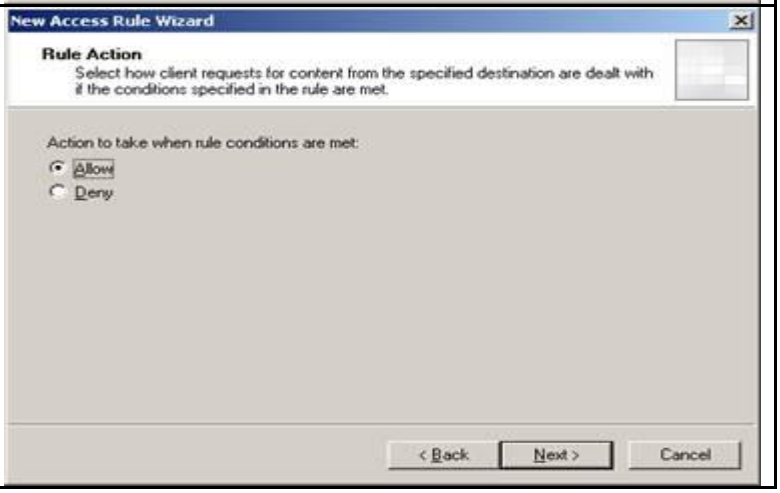
Khi cài ISA vào thì máy ISA Server sẽ trở thành Firewall. Lúc này ISA Server sẽ đứng ngoài cùng hệ thống mạng, chịu trách nhiệm giám sát việc truy xuất ra ngoài cũng như truy cập từ bên ngoài vào của toàn bộ hệ thống mạng. Giờ đây việc Publish các Web, FTP Server sẽ không Publish trực tiếp nữa mà thông qua ISA Server.

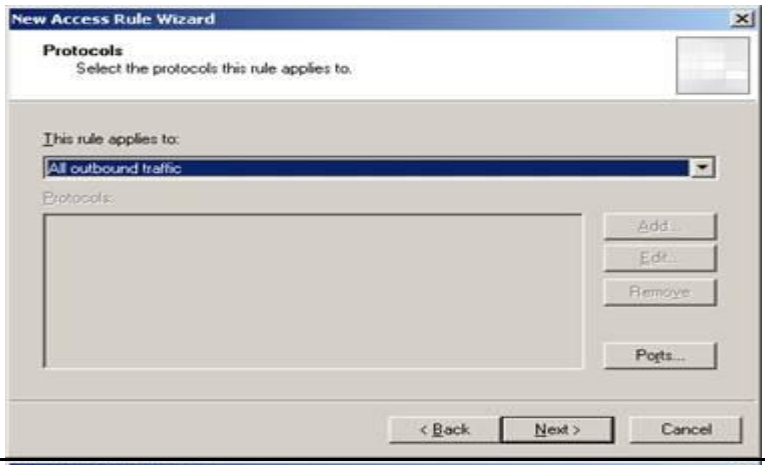
Khi bên ngoài yêu cầu truy cập Website của tổ chức, thì ISA sẽ lắng nghe và forward port 80 vào máy nào làm Web Server bên trong. Như vậy khi bị tấn công ISA sẽ hứng chịu toàn bộ các cuộc tấn công. Các Server sẽ trở nên an toàn hơn

Như vậy hệ thống của chúng ta sẽ được bảo mật hơn từ bên ngoài.

Cho phép các máy trong mạng LAN truy cập Internet

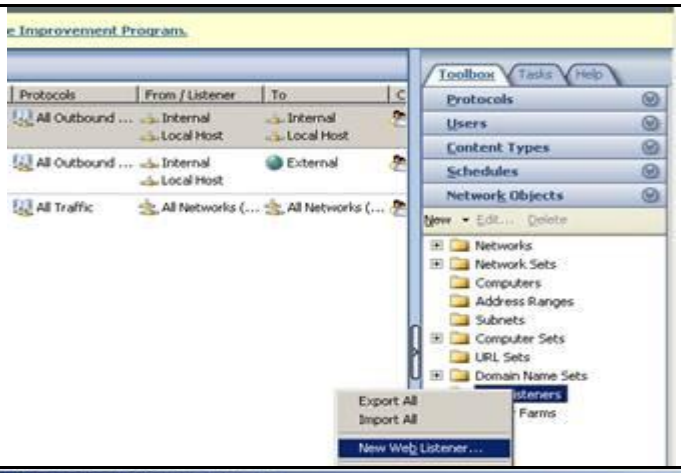
Tạo Access Rule cho phép Localhost và Internal truy cập lẫn nhau:

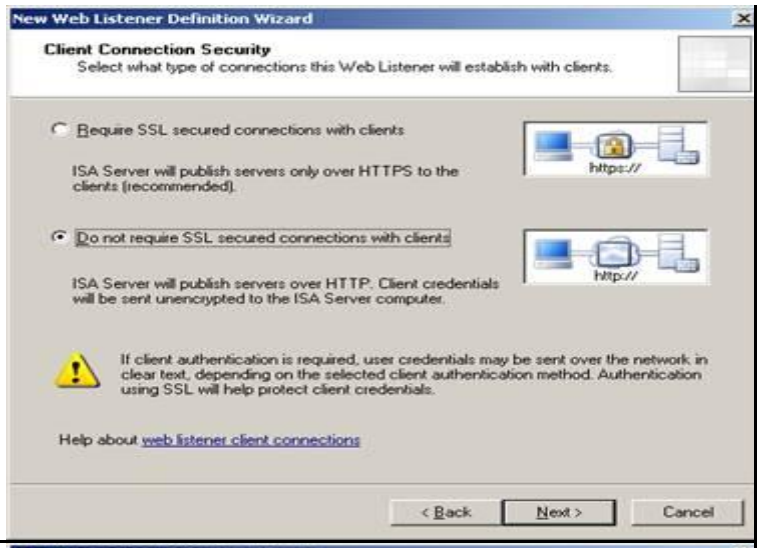
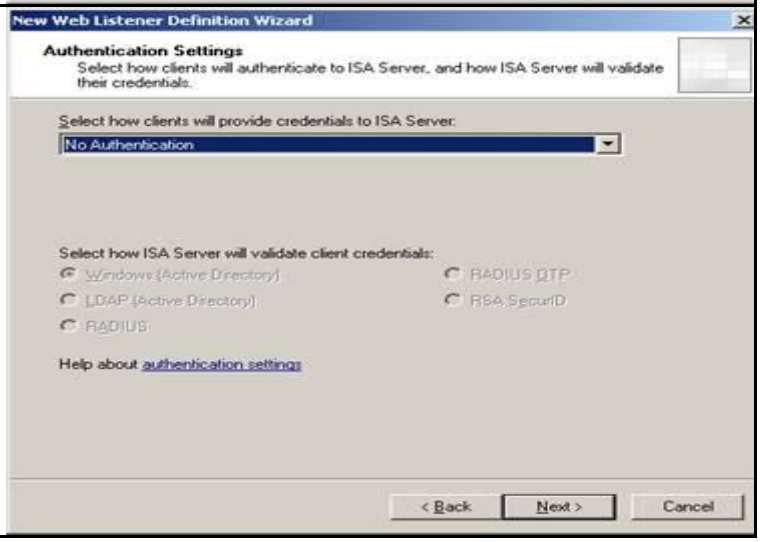
- Giao diện ISA Management: Click phải Firewall Policy → New → Access Rule	
- Đặt tên Access Rule: Internal-Localhost → Next	
- Chọn Allow → Next	

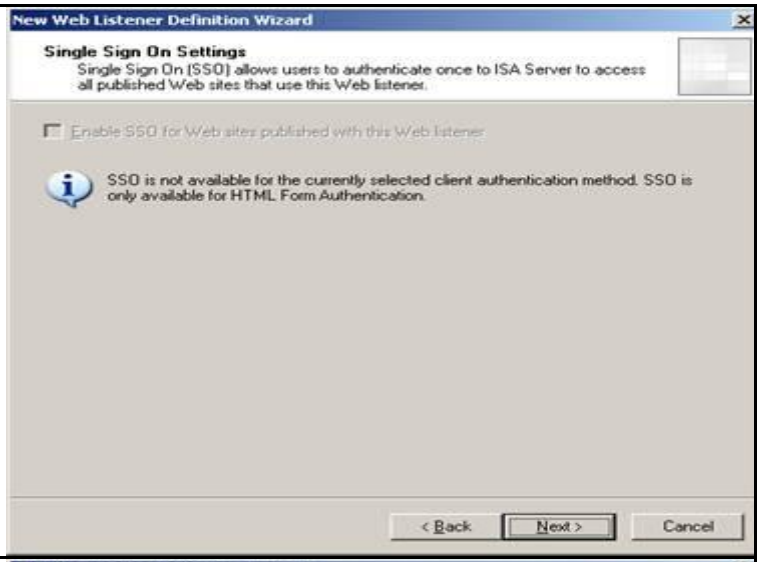
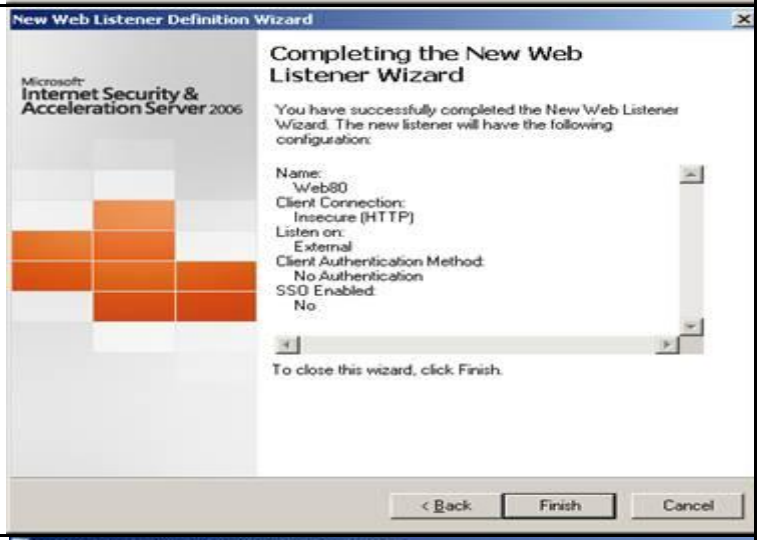
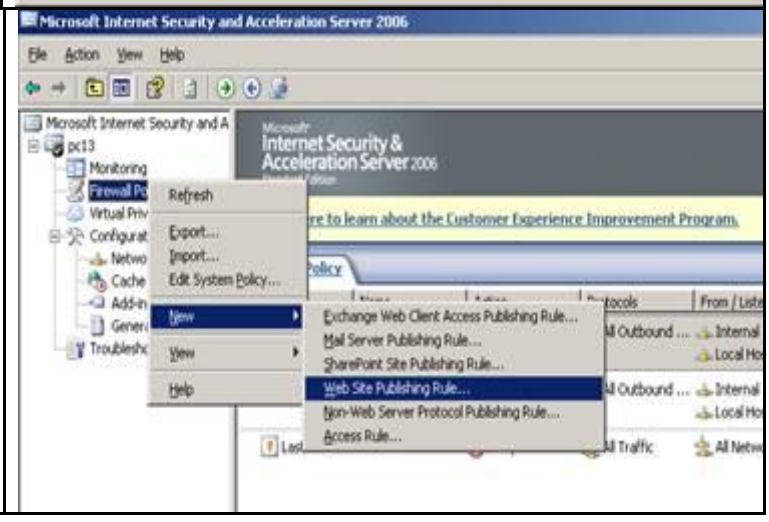
- Chọn All outbound traffic → Next	
- Nhấn Add - Double Click vào Internal - Double Click vào Localhost - Next	
- Next	

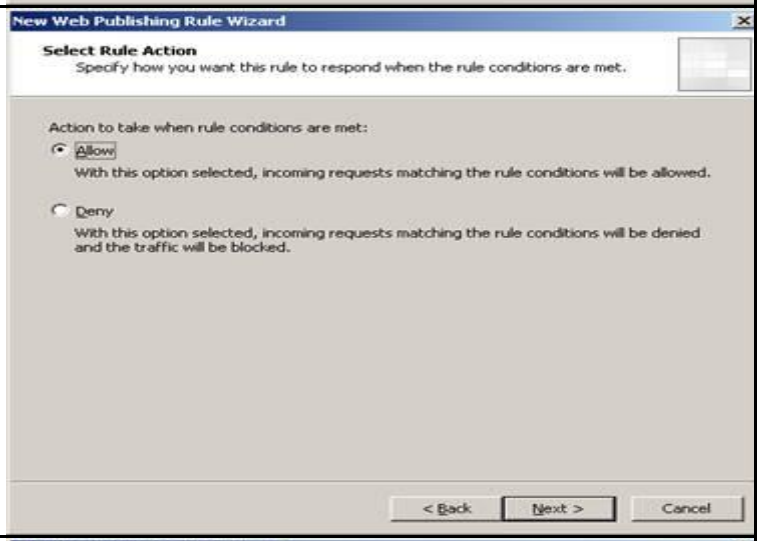
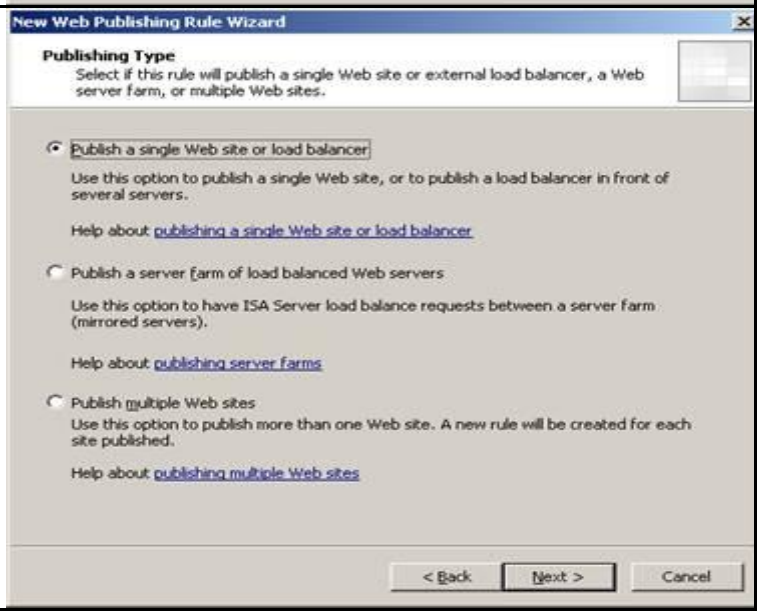
- Finish - Apply → OK	

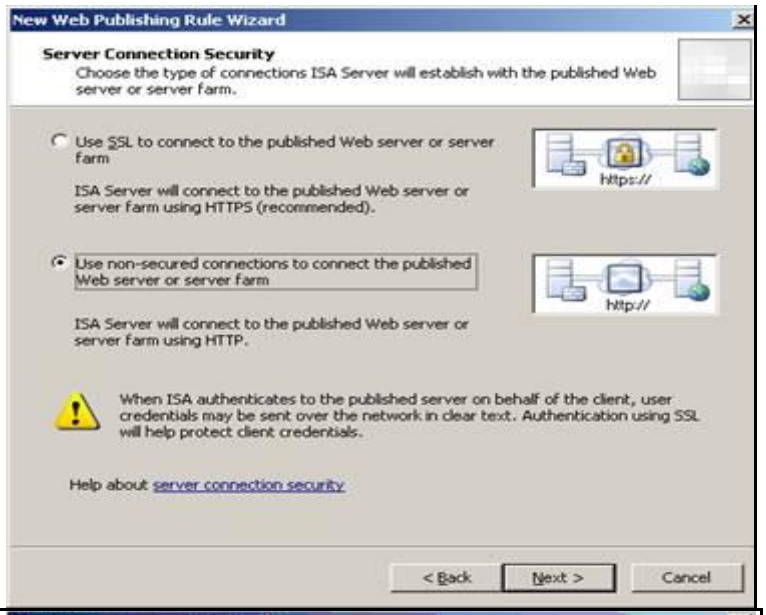
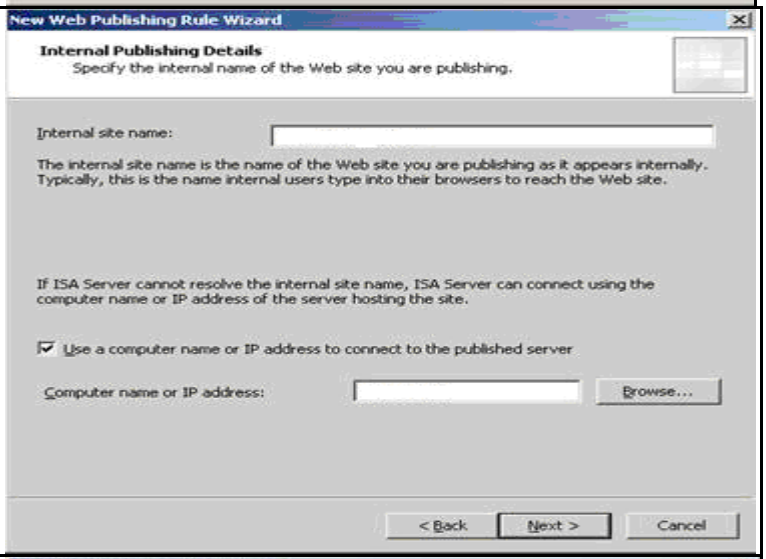
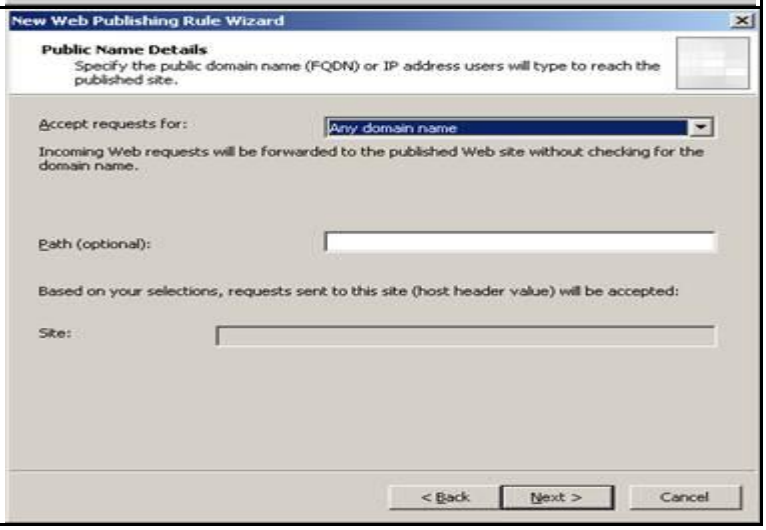
Tạo Publishing Rule để Publish Web Server:

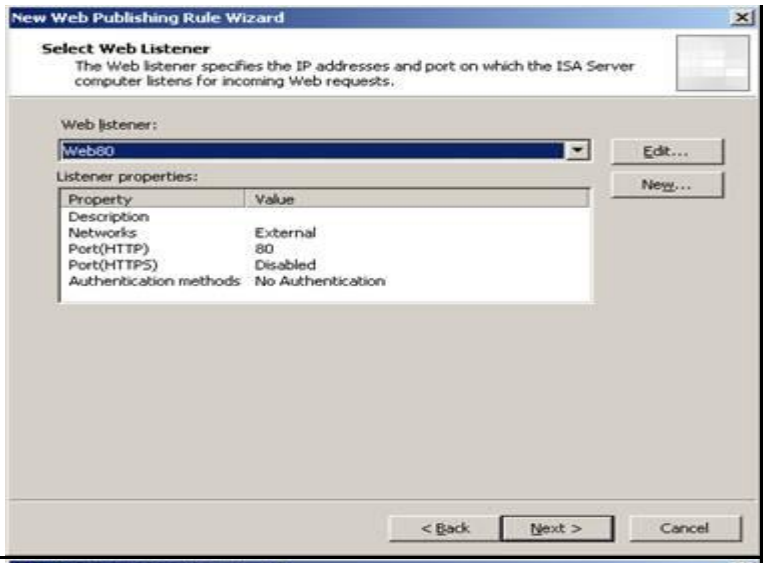
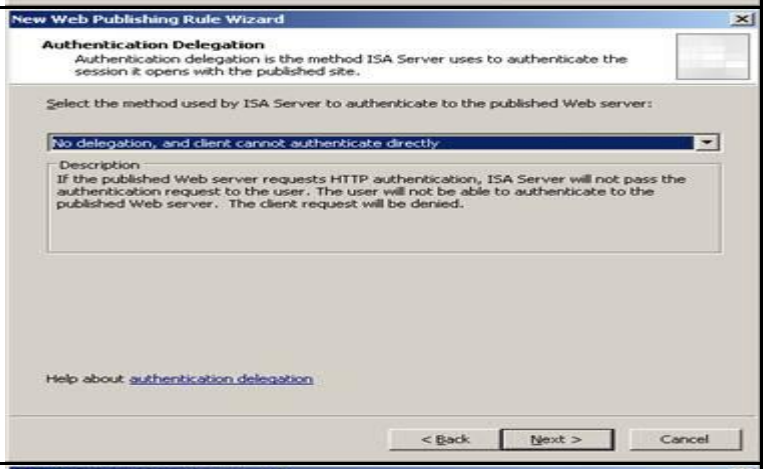
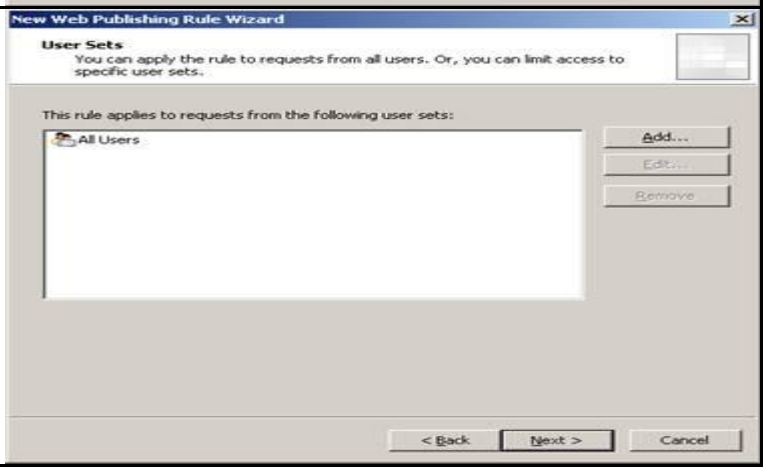
- Giao diện ISA Management: Firewall Policy → Toolbox → Network Objects → Click phải Web Listeners → New Web Listener	
- Đặt tên Web Listener là Web80 → Next	

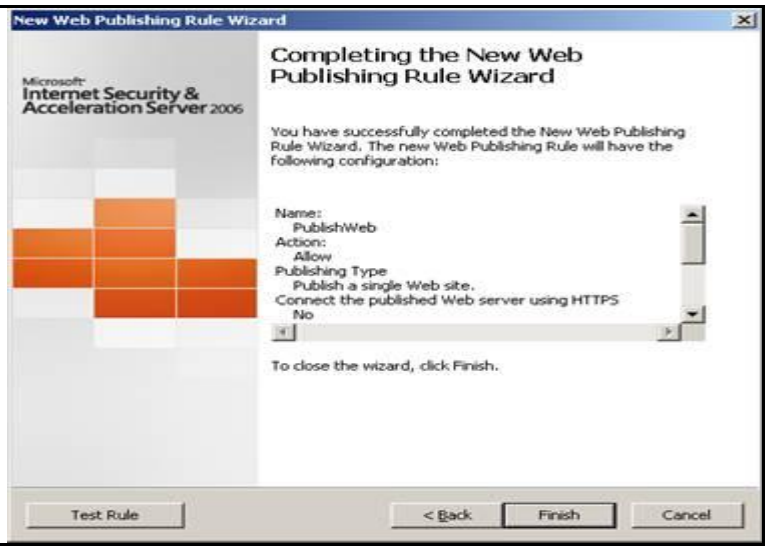
- Chọn Do not require SSL secured connetions with clients → Next	
- Đánh dấu mục chọn External → Next	
- Chọn No Authentication → Next	

Next	
- Finish	
- Click phải Firewall Policy → New → Web Site Publishing Rule	

- Đặt tên Rule: Publish Web → Next	
- Chọn Allow → Next	
- Chọn Publish a single Web site or load balancer → Next	

- Chọn Use non-secured connections to connect the published Web server or server farm → Next	
- Internal site name: đánh FQDN của máy Web Server (“”) - Đánh dấu chọn Use a computer name or IP address to connect to the published server - Computer name or IP address: đánh IP Web server (“”) - Next	
- Accept request for: chọn Any domain name → Next	

- Web Listener: Chọn Web80 → Next	
- Chọn No delegation, and client cannot authenticate directly → Next	
- Next	

- Finish → Apply → OK	

3.4. ĐỀ XUẤT MÔ HÌNH BẢO MẬT ÁP DỤNG CHO BỘ GTVT

Ứng dụng bảo vệ cơ sở dữ liệu trong hệ thống phần mềm quản lý dữ liệu, những thông tin quan trọng của Bộ, trung tâm CNTT sử dụng hệ quản trị CSDL Microsoft Access được phân quyền và bảo mật theo mật khẩu và mã hoá dữ liệu.

Áp dụng điều khiển truy nhập tự quyết trong hệ thống phần mềm quản lý của trung tâm CNTT

Điều khiển truy nhập tự quyết là phương thức giới hạn quyền truy nhập cho các đối tượng dựa trên việc xác nhận đối tượng của chủ thể hay nhóm chủ thể. Điều khiển truy nhập tự quyết là loại cơ chế điều khiển phổ biến nhất hiện nay được triển khai trên các hệ thống thông tin với việc cung cấp Username và Password cho từng người dùng trong các nhóm phân quyền khác nhau.

Các chủ thể và quyền hạn trong hệ thống

Dựa trên quá trình phân tích yêu cầu người dùng, trên cơ sở các yêu cầu đó hệ thống đưa ra các chức năng của các chủ thể. Hệ thống gồm ba chủ thể chính:

- Người quản lý: Trao quyền hoặc huỷ bỏ các quyền sử dụng hệ thống cho các nhân viên là Username và Password, và khách người truy cập website, quản lý các công việc cập nhật, sửa xoá, lưu trữ thông tin, cơ sở dữ liệu.

- Nhân viên: dành cho người sử dụng có quyền là Nhân viên trong văn phòng Bộ, là người sử dụng chính trong hệ thống. Nhân viên có nhiệm vụ và có quyền hạn sử dụng hệ thống trong phân vùng mà người quản lý cấp quyền, như được cấp tài khoản truy cập website của Bộ GTVT , truy cập, cập nhật CSDL, trao đổi mail…và được bảo vệ tính riêng tư

- Khách là người không thuộc cơ quan Bộ, có quyền truy cập vào website tra cứu thông tin, và khách cũng chỉ được sử dụng trong phân vùng cho phép (phân vùng phi quân sự DMZ "DeliMitary Zone")

Xác lập cơ chế điều khiển truy cập tự quyết

Đối với mỗi đối tượng, một người dùng hay một nhóm người dùng có xác nhận để cấp phát hay huỷ bỏ quyền truy nhập tới đối tượng đó. ". Điều khiển truy nhập MAC chủ yếu dựa trên xác nhận của người dùng và đối tượng.

Ma trận điều khiển truy nhập, chứa tên chủ thể trong các hàng, và tên đối tượng trong các cột. Mỗi giao điểm chỉ định kiểu truy nhập của người dùng đối với đối tượng đó. Trong đó các hàng thể hiện người dùng hệ thống, các cột biểu diễn đặc quyền của đối tượng lên chủ thể. Quyền truy nhập mô tả các thao tác nhất định mà chủ thể có thể thực hiện trên đối tượng.

Insert – chèn: chèn một bộ của đối tượng

Select - chọn: duyệt các bộ

Delete – xoá: xoá bộ của đối tượng

Update - cập nhật: thay đổi nội dung trong các bộ

Grant – trao quyền: trao quyền truy nhập đối tượng

Cơ chế điều khiển truy nhập được thông qua các chức năng của các hệ quản trị CSDL Microsoft Access. Bảng truy nhập của các chủ thể trong hệ thống quản lý đào tạo được thể hiện tổng quát hoá với cá chức năng sau:

Bảng 4.1. Quản lý dữ liệu hệ thống

Chủ thể	Select	Insert	Update	Delete	Grant
Người quản lý	✓	✓	✓	✓	✓
Nhân viên					
Khách					

Bảng 4.1. Quản lý nhân viên

Chủ thể	Select	Insert	Update	Delete	Grant
Người quản lý	✓	✓	✓	✓	✓
Nhân viên					
Khách					

Bảng 4.1. Quản lý khách

Chủ thể	Select	Insert	Update	Delete	Grant
Người quản lý	✓	✓	✓	✓	✓
Nhân viên					
Khách					

Bảng 4.1. Báo cáo thống kê

Chủ thể	Select	Insert	Update	Delete	Grant
Người quản lý	✓	✓	✓	✓	✓
Nhân viên					
Khách					

Áp dụng điều khiển truy nhập bắt buộc vào hệ thống

Xác định chủ thể, phân hạng an ninh

Điều khiển truy nhập bắt buộc MAC thiết lập dựa trên nhãn an ninh của các chủ thể và các đối tượng. Mức rõ clear(S) với chủ thể S, phân hạng class(O) với đối tượng O. Quyền truy nhập dựa theo hai thuộc tính:

- Thuộc tính đơn giản:chủ thể S có quyền đọc đối tượng O khi clear(S)> class(S).
- Thuộc tính sao: Chủ thể S có quyền ghi đối tượng O khi clear(S)< class(S).

Hệ thống gồm ba chủ thể chính: người quản lý, nhân viên, khách

Phân tích các yêu cầu sử dụng thông tin của các chủ thể trong hệ thống, các thuộc tính được chỉ định thành các hãng an ninh được chỉ định theo thứ tự:

U<C<S<TS. Hệ thống nhãn được chỉ định dựa trên chức năng và yêu cầu an ninh của hệ thống đối với từng chủ thể của hệ thống.

Trong đó:

U – Unclassified: mức an ninh ngầm định

C – Confident: mức an ninh thứ hai

S – Seret: mức an ninh thư ba

TS – TopSecret: mức an ninh thứ tư

Yêu cầu an ninh hệ thống

Hệ thống quản lý đào tạo đươc phân cấp theo từng khung nhìn dựa trên phân loại người dùng. Các khung nhìn được thiết lập trong hệ thống gồm có:

- Khung nhìn $View_1$: hiển thị của sổ truy nhập cho giáo vụ. Người có khung nhìn $View_1$ có thể truy nhập toàn CSDL.

- Khung nhìn $View_2$: Hiển thị thông tin cho các chủ thể là nhân viên.

- Khung nhìn $View_{3:}$ hiển thị của sổ truy nhập cho các chủ thể là khách.

3.5. ĐỀ XUẤT BIỆN PHÁP BẢO MẬT DỮ LIỆU ÁP DỤNG CHO BỘ GTVT

Trong thực tế, các thông tin mật của hệ thống có thể bị tiết lộ hoặc thay đổi thông qua các tập tin *.mdb một cách khá đơn giản với các sản phẩm của Microsoft được dùng chung dữ liệu. Những việc này thật đơn giản với những ai chỉ cần có chút kiến thức về tin học và biết được file cơ sở dữ liệu đặt ở đâu trong hệ thống.

Không những thế, hệ thống có thể dễ dàng bị đăng nhập thông qua việc lấy thông tin bằng cách làm giả file mật khẩu….

Bảo mật sơ sở dữ liệu bảng mã hoá

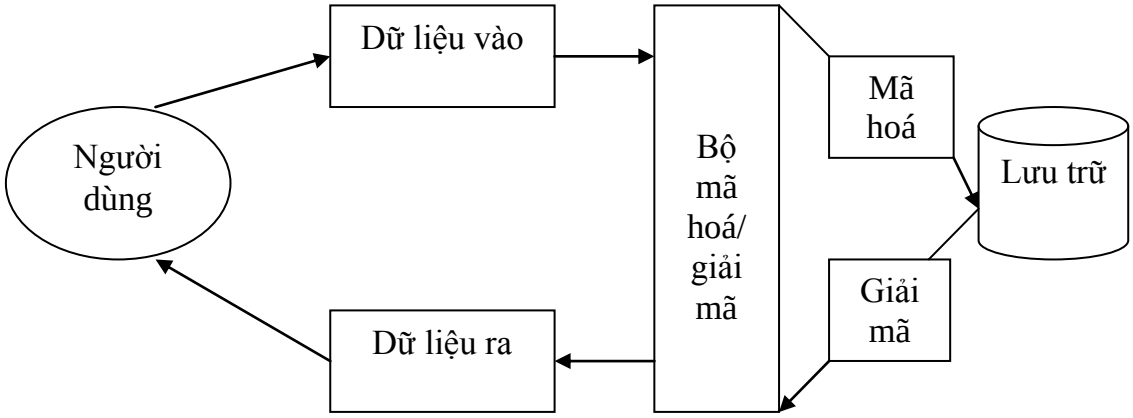
Như đã nêu file chứa mật khẩu có thành phần mật khẩu được mã hoá do vậy không đọc được mật khẩu một cách dễ dàng. Muốn giải mã để tìm được mật khẩu chúng ta cần phải biết thuật toán và khoá được dùng khi mã hoá. Với số lượng thuật toán mã hoá đã biết thì việc tìm kiếm theo phương pháp vét cạn là không thực tế.

Như vậy nếu dữ liệu được lưu trong tập tin *.mdb đã được mã hoá bằng một thuật toán mã hoá bất kỳ thì rõ ràng việc truy nhập vào CSDL trực tiếp không thông qua chương trình sẽ không có ý nghĩa vì không đọc được nội dung thực của thông tin được lưu trữ.

Tuy nhiên hệ thống vẫn bị xâm phạm nếu làm giả được mật khẩu truy nhập vào hệ thống. Bởi vì trong phiên làm việc dữ liệu được thể hiện ở dạng không mã hoá để người dùng có thể hiểu được.

Từ các phân tích trên đề xuất việc mã hoá như sau:

Toàn bộ CSDL sẽ được mã hoá bằng một khoá do người quản trị lựa chọn tương tự như cơ chế sử dụng mật khẩu. Trước khi chương trình làm việc với CSDL thông tin được lưu trữ sẽ được giải mã và khi kết thúc phiên làm việc thông tin lại được mã hoá trước khi lưu trữ. Với hệ thống đề xuất việc bổ sung modul mã hoá và giải mã dữ liệu trước và sau khi sử dụng dữ liệu. Sơ đồ đề xuất gồm:

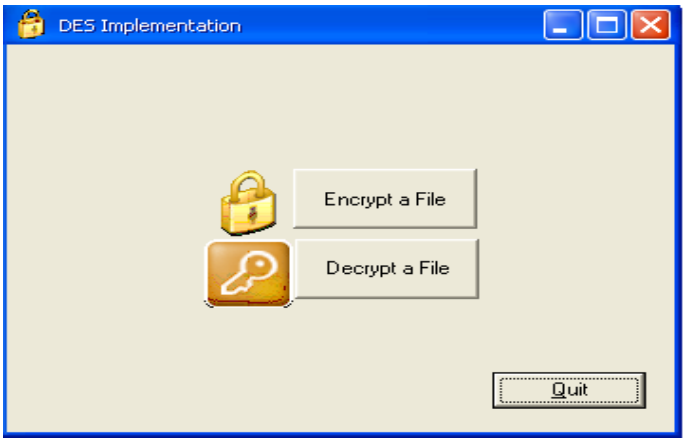


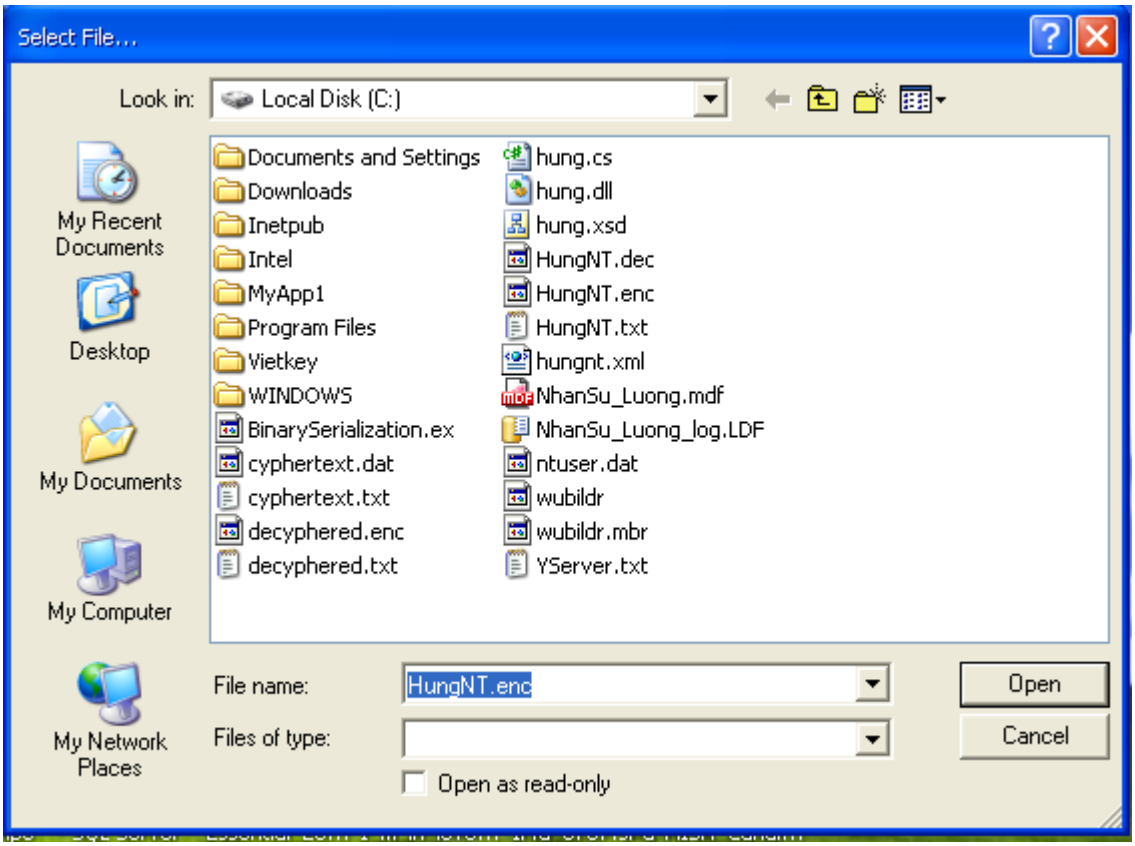
Chương trình demo mô hình mã hóa giải mã bằng thuật toán DES

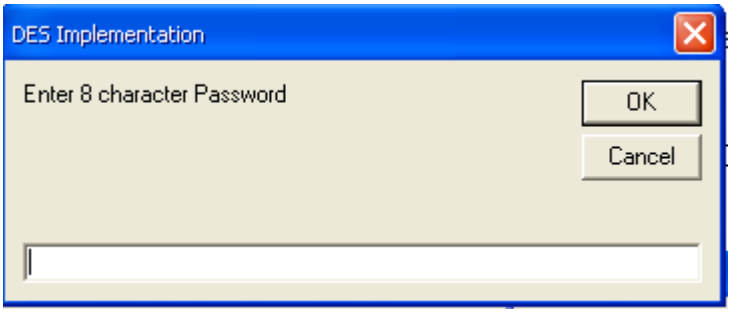
Môi trường cài đặt:

- Ngôn ngữ lập trình Microsoft Visual Basic 6.0
- Hệ điều hành Windows XP
- Máy tính Petium III, CPU 550 Hz, 128 MB RAM

Một số giao diện hệ thống




Select File...
Look in:
Local Disk (C:)
My Recent Documents
Desktop
My Documents
My Computer
My Network Places
Documents and Settings
Downloads
Inetpub
Intel
MyApp1
Program Files
Vietkey
WINDOWS
BinarySerialization.ex
cyphertext.dat
cyphertext.txt
decyphered.enc
decyphered.txt
hung.cs
hung.dll
hung.xsd
HungNT.dec
HungNT.enc
HungNT.txt
hungnt.xml
NhanSu_Luong.mdf
NhanSu_Luong_log.LDF
ntuser.dat
wubildr
wubildr.mbr
YServer.txt
File name:
HungNT.enc
Files of type:
Open as read-only
Open
Cancel


DES Implementation
Enter 8 character Password
OK
Cancel

MỘT SỐ ĐOẠN MÃ CHÍNH CỦA CHƯƠNG TRÌNH

CHUONG TRINH MA HOA DES

```
Private Sub encrypt_btn_Click()
round_no = 1
str1 = Text3.Text
For i = 1 To Len(str1)
asc_code = (convert_to_binary(Asc(Mid$(str1, i, 1))))
str3 = LTrim$(Str(asc_code))
diff = 9 - Len(str3)
If diff > 1 Then
   For j = 1 To diff - 1
      str3 = "0" + str3
   Next j
End If
str2 = str2 + str3
Next i
input_key = str2
MsgBox input_key + Str(Len(input_key))
str1 = Text1.Text
str2 = ""
For i = 1 To Len(str1)
  asc_code = (convert_to_binary(Asc(Mid$(str1, i, 1))))
str3 = LTrim$(Str(asc_code))
diff = 9 - Len(str3)
If diff > 1 Then
For j = 1 To diff - 1
str3 = "0" + str3
```

```
Next j
End If
str2 = str2 + str3
Next i
plain_text = str2
str4 = plain_text
ip
For i = 1 To 32
l_block = l_block + Mid$(plain_text, i, 1)
r_block = r_block + Mid$(plain_text, 32 + i, 1)
Next i
permuted_choice_1
'*********************************************************
generate_sub_keys
While (round_no <= 16)
plain_text = r_block
Expansion_permutation
str3 = vbNullString
For i = 1 To 48
      If (Mid$(plain_text, i, 1) = Mid$(sub_key(round_no), i, 1)) Then
   str3 = str3 + "0"
   Else
   str3 = str3 + "1"
   End If
Next i
counter = 1
tmp_str2 = vbNullString
plain_text = str3
```

```
For i = 1 To 48 Step 6
str2 = Mid$(plain_text, i, 6)
tmp_str1 = Mid$(str2, 1, 1)
tmp_str1 = tmp_str1 + Mid$(str2, 6, 1)
row_no = convert_to_decimal 'converts the contents in tmp_str1 to decimal...
tmp_str1 = Mid$(str2, 2, 4)
col_no = convert_to_decimal 'converts the contents in tmp_str1 to decimal...
j = row_no * 16 + (col_no)
j = (j * 2) + 1
j = convert_to_binary(Val(Mid$(s_box(counter), j, 2)))
str3 = LTrim$(Str(j))
diff = 5 - Len(str3)
If diff > 1 Then
For j = 1 To diff - 1
str3 = "0" + str3
Next j
End If
tmp_str2 = tmp_str2 + str3
counter = counter + 1
Next i
plain_text = tmp_str2
'*******************************************************
str3 = vbNullString
For i = 1 To 32
   If (Mid$(l_block, i, 1) = Mid$(plain_text, i, 1)) Then
   str3 = str3 + "0"
   Else
   str3 = str3 + "1"
```

```
    End If
Next i
l_block = r_block
r_block = str3
round_no = round_no + 1
Wend
tmp_str1 = r_block
r_block = l_block
l_block = tmp_str1
plain_text = l_block + r_block
ip_inverse
str2 = vbNullString
str3 = vbNullString
For i = 1 To 64 Step 8
tmp_str1 = Mid$(plain_text, i, 8)
str2 = LTrim$(Str(convert_to_decimal))
Text2.Text = Text2.Text + Chr(Val(str2))
Next i
MsgBox str4 + Str(Len(str4)) + vbCrLf + plain_text + Str(Len(plain_text)) + vbCrLf + str3
End Sub
```

CHƯƠNG TRÌNH GIẢI MÃ DES

```
Private Sub decrypt_btn_Click()
round_no = 16
str1 = vbNullString
str2 = vbNullString
str3 = vbNullString
str4 = vbNullString
```

```
l_block = vbNullString
r_block = vbNullString
c_block = vbNullString
d_block = vbNullString
plain_text = vbNullString
input_key = vbNullString
tmp_str1 = vbNullString
tmp_str2 = vbNullString
str1 = Text3.Text
For i = 1 To Len(str1)
asc_code = (convert_to_binary(Asc(Mid$(str1, i, 1))))
str3 = LTrim$(Str(asc_code))
diff = 9 - Len(str3)
If diff > 1 Then
   For j = 1 To diff - 1
      str3 = "0" + str3
   Next j
End If
str2 = str2 + str3
Next i
input_key = str2
MsgBox input_key + Str(Len(input_key))
str1 = Text2.Text
str2 = ""
For i = 1 To Len(str1)
asc_code = (convert_to_binary(Asc(Mid$(str1, i, 1))))
str3 = LTrim$(Str(asc_code))
diff = 9 - Len(str3)
```

```
If diff > 1 Then
For j = 1 To diff - 1
str3 = "0" + str3
Next j
End If
str2 = str2 + str3
Next i
plain_text = str2
str4 = plain_text
ip
For i = 1 To 32
l_block = l_block + Mid$(plain_text, i, 1)
r_block = r_block + Mid$(plain_text, 32 + i, 1)
Next i
permuted_choice_1
generate_sub_keys
While (round_no >= 1)
plain_text = r_block
Expansion_permutation
str3 = vbNullString
For i = 1 To 48
   If (Mid$(plain_text, i, 1) = Mid$(sub_key(round_no), i, 1)) Then
   str3 = str3 + "0"
   Else
   str3 = str3 + "1"
   End If
Next i
counter = 1
```

```
tmp_str2 = vbNullString
plain_text = str3
For i = 1 To 48 Step 6
str2 = Mid$(plain_text, i, 6)
tmp_str1 = Mid$(str2, 1, 1)
tmp_str1 = tmp_str1 + Mid$(str2, 6, 1)
row_no = convert_to_decimal 'converts the contents in tmp_str1 to decimal...
tmp_str1 = Mid$(str2, 2, 4)
col_no = convert_to_decimal 'converts the contents in tmp_str1 to decimal...
j = row_no * 16 + (col_no)
j = (j * 2) + 1
j = convert_to_binary(Val(Mid$(s_box(counter), j, 2)))
str3 = LTrim$(Str(j))
diff = 5 - Len(str3)
If diff > 1 Then
For j = 1 To diff - 1
str3 = "0" + str3
Next j
End If
tmp_str2 = tmp_str2 + str3
counter = counter + 1
Next i
plain_text = tmp_str2
permutation_P
'*******************************************************
str3 = vbNullString
For i = 1 To 32
   If (Mid$(l_block, i, 1) = Mid$(plain_text, i, 1)) Then
```

```
        str3 = str3 + "0"
        Else
        str3 = str3 + "1"
        End If
    Next i
    l_block = r_block
    r_block = str3
    round_no = round_no - 1
    Wend
    tmp_str1 = r_block
    r_block = l_block
    l_block = tmp_str1
    plain_text = l_block + r_block
    ip_inverse
    str2 = vbNullString
    str3 = vbNullString
    For i = 1 To 64 Step 8
    tmp_str1 = Mid$(plain_text, i, 8)
    str2 = LTrim$(Str(convert_to_decimal))
    Text1.Text = Text1.Text + Chr(Val(str2))
    Next i
    MsgBox str4 + Str(Len(str4)) + vbCrLf + plain_text + Str(Len(plain_text)) +
vbCrLf + str3
    End Sub
```

KẾT LUẬN

An toàn thông tin và các giải pháp an toàn đang là vấn đề đang được quan tâm và ngày càng được chú trọng hiện nay.Vì vậy nghiên cứu và đưa ra những giải pháp giải quyết vấn đề này hết sức cần thiết và phải được triển khai một các mạnh mẽ và hiệu quả.

Tại Việt Nam Bộ thông tin và truyền thông, đã và đang triển khai rất nhiều dự án nhằm xây dựng các hệ thống thông tin, vì sự phát triển chung nhằm đảm bảo tốt hơn một môi trường hoạt động trong lĩnh vực công nghệ thông tin một các an toàn và bền vững.

Trong quá trình làm luận văn tốt nghiệp, em đã không tránh khỏi những thiếu sót, em cố gắng tìm hiểu các hệ thống thông tin, nghiên cứu, đưa ra các giải pháp an toàn và các ứng dụng cho các lĩnh vực của công nhên thông tin hiện nay. Kính mong thầy cô giúp đỡ cho chương trình của em ngày càng hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

1. Tài liêu điện tử Lý thuyết mật mã & an toàn bảo mật thông tin của Phan Đình Diệu khoa công nghệ thông tin –Đại học quốc gia Hà Nôi – 2002
2. An toàn bảo mật thông tin của Lê Thụy khoa công nghệ thông tin – Đại học dân lập Hải Phòng.
3. Website của Bộ giao thông vận tải: www.mt.gov.vn .
4. An toàn bảo mật hệ thống thông tin, Nguyễn Huy Công, 2004
5. William Stallings, Cryptography and Netword Security, Pearson Education International, 2000.
6. Cryptography: Theory and Practice Douglas R.Stinson, CRC Press 1995.
7. Computer Security , Lawrie Brown
8. Tyson Condie, *Unstructured P2P Networks*