ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

BÙI THÁI LONG

NGHIÊN CỨU MỘT SỐ PHƯƠNG PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN TRONG MẠNG MÁY TÍNH

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01 01

Người hướng dẫn khoa học

PGS.TS Trịnh Nhật Tiến

Thái Nguyên – 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này của tự bản thân tôi tìm hiểu, nghiên cứu dưới sự hướng dẫn của PGS.TS Trịnh Nhật Tiến. Các chương trình thực nghiệm do chính bản thân tôi lập trình, các kết quả là hoàn toàn trung thực. Các tài liệu tham khảo được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

Bùi Thái Long

LỜI CẢM ƠN

Tôi xin bày tỏ lời cảm ơn chân thành tới tập thể các thầy cô giáo Viện công nghệ thông tin – Viện Hàn lâm Khoa học và Công nghệ Việt Nam, các thầy cô giáo Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên đã dạy dỗ chúng tôi trong suốt quá trình học tập chương trình cao học tại trường.

Đặc biệt tôi xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo PGS.TS Trịnh Nhật Tiến, Trường Đại học Công nghệ – Đại học Quốc gia Hà Nội đã quan tâm, định hướng và đưa ra những góp ý, gợi ý, chỉnh sửa quý báu cho tôi trong quá trình làm luận văn tốt nghiệp.

Cuối cùng, tôi xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với em trong suốt quá trình làm luận văn tốt nghiệp.

Thái Nguyên, ngày tháng năm 2015

HỌC VIÊN

Bùi Thái Long

MỤC LỤC

DANH SÁCH KÍ HIỆU, TỪ VIẾT TẮT

Viết tắt	Viết đầy đủ
CERT	Computer Emergency Reponse Team
CIAC	Department of Energy Computer Incident Advisory Capability
DARPA	Defense Advanced Research Projects Agency
FIRST	The Forum of Incident Response and Security Teams
PKI	Public Key Infrasture
RPC	Remote Procedure Call
SSL/TLS	Secure Socket layer/Transport Layer Security
VPN	Virtual Private Network

DANH MỤC CÁC HÌNH ẢNH

LỜI MỞ ĐẦU

1. Lý do lựa chọn đề tài.

Trong những năm gần đây, sự bùng nổ của cách mạng thông tin đang diễn ra nhanh chóng trên phạm vi toàn thế giới. Sự phổ biến rộng rãi của Internet đã kết nối mọi người trên thế giới lại với nhau, trở thành công cụ không thể thiếu, làm tăng hiệu quả làm việc, tăng sự hiểu biết, trao đổi, cập nhật các thông tin nhanh chóng và tiện lợi.

Tuy nhiên, Internet là một mạng mở, nó cũng chứa đựng nhiều hiểm họa đe dọa hệ thống mạng, hệ thống máy tính, tài nguyên thông tin cá nhân của các tổ chức cá nhân hay doanh nghiệp. Như những tin tức quan trọng nằm ở kho dữ liệu hay trên đường truyền có thể bị tấn công, xâm nhập và lấy cắp thông tin. Do vậy, nảy sinh yêu cầu nghiên cứu các phương pháp bảo đảm an toàn thông tin như: Kiểm soát các lỗ hổng an ninh mạng, kiểm soát các dạng tấn công mạng nhằm mục đích ngăn chặn hạn chế các rủi ro đối với thông tin trong mạng máy tính.

Chính vì nhận thấy nhiệm vụ bảo vệ an toàn thông tin trong mạng máy tính, đặc biệt ở Việt Nam nên Em đã chọn đề tài "Nghiên cứu một số phương pháp bảo đảm an toàn thông tin trong mạng máy tính", đề tài này theo Tôi được biết là đã có một số Tổ chức, Doanh nghiệp, Viện, Trường Đại Học… nghiên cứu nhưng vẫn dừng ở một mức độ nhất định vì vậy Tôi vẫn quyết tâm nhận đề tài này với các nhiệm vụ cần đi sâu là nghiên cứu, đề xuất các giải pháp an toàn thông tin dựa trên kiến trúc tổng quan của mô hình an toàn thông tin trong mạng máy tính và vận dụng cơ sở lý thuyết mật mã ứng dụng vào an toàn thông tin.

2. Đối tượng và phạm vi nghiên cứu

- Đề tài nghiên cứu các phương pháp để thực hiện nhiệm vụ bảo mật và an toàn thông tin trong mạng máy tính, quá trình thực hiện và các kiến thức khoa học và thuật toán liên quan như: Xác thực, bảo mật, bảo toàn dữ liệu, mật mã, chữ ký số …

- Áp dụng các kết quả nghiên cứu để triển khai hệ thống bảo đảm an toàn thông tin trong mạng máy tính.

3. Hướng nghiên cứu của đề tài

**** Về lý thuyết:***

+ Nghiên cứu các hiểm họa về mất an toàn thông tin trong mạng máy tính.

+ Nghiên cứu một số phương pháp bảo vệ thông tin trong mạng máy tính.

+ Nghiên cứu về công nghệ mât mã, công nghệ mạng riêng ảo, tường lửa.

+ Giải pháp kiểm soát và xử lý các lỗ hổng trên mạng máy tính.

+ Giải pháp kiểm soát và xử lý các dạng tấn công mạng máy tính.

**** Về thực nghiệm:***

+ Thực hiện xây dựng thử nghiệm bảo vệ thông tin bằng phương pháp mã hóa.

+ Thực hiện xây dựng thử nghiệm ứng dụng kiểm soát lỗi truyền tin nhập thông tin bằng chữ ký số và mã hóa.

4. Những nội dung nghiên cứu chính

Chương 1: Các hiểm họa về an toàn thông tin trên mạng máy tính.

Chương 2: Một số phương pháp bảo vệ thông tin trên mạng máy tính.

Chương 3: Thử nghiệm ứng dụng bảo vệ thông tin trên mạng máy tính.

Chương 1: CÁC HIỂM HỌA VỀ AN TOÀN THÔNG TIN TRÊN MẠNG MÁY TÍNH.

1.1. VẤN ĐỀ AN NINH MẠNG MÁY TÍNH.

1.1.1. An ninh hệ thống.

Các hệ thống máy tính được cấu thành từ các thiết bị phần cứng như bộ vi xử lý, đơn vị điều khiển vào ra, các thiết bị ngoại vi (đĩa cứng, máy in...) và hệ điều hành với các thành phần lõi hệ điều hành, hệ thống tệp, các tiến trình hệ thống, các dịch vụ hệ thống. Tất cả các thành phần nêu trên đều có thể bị đột nhập hay bị lợi dụng khai thác bởi các kẽ hở của chính bản thân các thành phần đó nhằm làm suy yếu và tê liệt một phần hoặc toàn bộ hệ thống

1.1.1.1. Các tấn công vào phần cứng.

Các tấn công vào phần cứng dựa trên lỗi của chính bản thân phần cứng. Đây là lỗi của thiết kế phần cứng và kẻ tấn công có thể lợi dụng những lỗi này để tấn công hệ thống.Ví dụ: mặc dù đã được cải tiến và phát triển rất lâu, bộ vi xử lý Pentium của Intel vẫn còn có lỗi. Chỉ cần thực hiện một đoạn mã đặc biệt là có thể làm cho hệ thống bị tê liệt hoàn toàn, bất kể hệ điều hành được sử dụng có ưu việt đến đâu và hoạt động ở chế độ bảo vệ nào.

1.1.1.2. Các truy nhập không được phép.

Cách dễ nhất để vào một hệ thống máy tính là thông qua hình thức đăng nhập "Login". Kẻ tấn công có nhiều cách để truy nhập bất hợp pháp vào hệ thống. Các kiểu này có thể là:

a/. Mạo danh người sử dụng để yêu cầu thay đổi mật khẩu.

b/. Các phép toán đơn giản (thử một tên tài khoản và các kết hợp của mật khẩu cho đến khi có được một tài khoản hoạt động); hoặc

c/. Bằng một cách phức tạp mà không cần biết tên tài khoản và mật khẩu.

1.1.1.3. Lỗi hệ thống và các trình ẩn nấp.

Sau đây là mô tả một số lỗi hệ thống thường gặp.

- Lỗi của cơ chế xác thực

Rất nhiều cuộc tấn công xuất phát từ sự hỏng cơ chế xác thực của hệ thống. Ví dụ: quá trình kiểm tra địa chỉ nguồn IP có thể hoạt động tốt trong một tình huống nào đó, nhưng những kẻ tấn công có thể dùng trình "portmapper" để gửi lại các yêu cầu. Trong trường hợp đó, dịch vụ nền tảng cuối cùng đã bị lừa, bản tin được gửi đến máy dịch vụ xuất hiện dường như từ địa chỉ nguồn nội bộ, nhưng thực ra nó xuất phát từ nơi nào đó khác.

Xác thực dựa trên địa chỉ IP cũng có thể bị hỏng nếu hệ thống gửi yêu cầu xác thực không đáng tin cậy. Có lúc, cơ chế xác thực hỏng do các giao thức không mang thông tin đúng đắn. Cả TCP và IP đều không định dạng người gửi; các giao thức như X11 và *rsh* phải tự lấy địa chỉ nguồn IP mà không biết có tin tưởng được địa chỉ đó không.

- Lỗi các giao thức

Đây là trường hợp các lỗi xuất hiện trong bản thân các phần mềm thực hiện giao thức, từ chối các ứng dụng và từ chối công việc thường nhật.

Một ví dụ: các tấn công nhờ "số tuần tự IP". Vì không đủ số ngẫu nhiên trong quá trình tạo "số tuần tự TCP ban đầu" cho một kết nối TCP nên có thể gây ra kẽ hở cho kẻ tấn công lừa địa chỉ nguồn. Nói đúng hơn, các số tuần tự TCP không được thiết kế để chống lại các tấn công thâm hiểm. Các giao thức khác dựa trên số tuần tự đều có thể bị tấn công bằng cùng một phương thức, bao gồm cả dịch vụ tên miền DNS và dịch vụ thực hiện tiến trình từ xa RPC (Remote Procedure Call)

- Rò rỉ thông tin người sử dụng

Hầu hết các dịch vụ đều cung cấp một vài thông tin về người sử dụng dịch vụ đó.

Thông thường, đây là yêu cầu của chính người dùng dịch vụ này. Các thông tin đó có thể là mục tiêu của các tình báo thương mại hay nó có thể giúp đỡ đột nhập hệ thống. Dịch vụ "finger" là một ví dụ. Các thông tin mà nó cung cấp có ích rất nhiều cho các kẻ mò mật khẩu hoặc mạo danh người sử dụng.

- Từ chối dịch vụ

Các yêu cầu được gửi đến máy dịch vụ quá nhiều có thể gây nên tình trạng từ chối dịch vụ. Nguyên nhân ở đây là do các máy dịch vụ phải sản sinh nhiều tiến trình con và hệ thống phải cấp phát bộ nhớ và vùng đệm cho chúng. Đến một lúc, tài nguyên hệ thống hết và dịch vụ trở nên "trơ" với các yêu cầu, nghĩa là nó không trả lời các yêu cầu từ người dùng.

Làm tràn ngập mạng để dẫn đến từ chối dịch vụ là cách đơn giản và thông thường. Những kẻ tấn công thông minh hơn còn có thể làm tê liệt dịch vụ, định hướng lại hay thay thế các dịch vụ.

1.2. HIỂM HỌA VỀ AN NINH MẠNG.

Ta xem xét khía cạnh an ninh của mạng dựa trên công nghệ Internet, sử dụng bộ giao thức TCP/IP:

TCP/IP không có cơ chế xác thực đối với mỗi số liệu, do đó kẻ tấn công có thể dùng các gói số liệu giả mạo đánh lừa các hệ thống.

Bản thân các giao thức thành phần trong bộ giao thức TCP/IP đều được thiết kế để làm việc với một loại gói số liệu nhất định, với một thủ tục thiết lập kết nối (thủ tục bắt tay) và trao đổi số liệu nhất định. Do đó, nếu các giao thức thành phần này phải làm việc ở một chế độ khác hay với một loạt giả mạo khi thiết lập kết nối và trao đổi số liệu thì rất có thể chúng ta sẽ suy yếu hay là sụp đổ cả hệ TCP/IP của hệ thống.

Các mô tả một số ví dụ về hiểm họa tấn công hệ thống.

1.2.1. Sử dụng gói số liệu quá lớn (Ping of Death)

Thực tế cho thấy, nhiều hệ thống có các phản ứng bất bình thường (ví dụ: hệ hoạt động suy sụp, bị treo hoặc bị khởi động lại) khi nhận được gói IP quá lớn. Cách thông thường nhất để lợi dụng điểm yếu này là thông qua gói ICMP được tạo ra bởi lệnh *ping* trong các hệ thống. ICMP là một giao thức hỗ trợ điều khiển trong bộ giao thức TCP/IP.

Thông thường, các lệnh *ping* đều tạo các gói số liệu có chứa 8 byte thông tin tiêu đề của ICMP và khoảng 64 byte số liệu. Nhưng các lệnh ping còn cho phép người dung tạo các gói lớn hơn nếu họ muốn. Một gói IP có độ dài lớn hơn 65536 byte được coi là không hợp lệ. Khi gói này được tạo ra và truyền đến đích nó sẽ bị phân mảnh trên đường truyền. Khi các gói đến đích, chúng sẽ được tái lập thành gói ban đầu, với độ lớn 65536 bytes và làm tràn vùng đệm trên nhiều hệ thống.

1.2.2. Giả địa chỉ IP

Thông thường, đối với một mạng dùng riêng, có một hệ thống tường lửa (firewall) hay bộ lọc gói (parket filter) dùng ngăn chặn việc trao đổi số liệu không được phép giữa mạng dùng riêng và mạng bên ngoài.

Trong trường hợp một hoặc nhiều máy thuộc mạng dùng riêng được “quy định” là tin cậy thì các dịch vụ đi từ những máy này đến máy đích không cần qua bất cứ

trình xác thực nào. Công việc này cho phép giảm thiểu các quá trình xác thực truy nhập vào các máy trong cùng mạng nội bộ.

Nếu kẻ tấn công bên ngoài gửi các gói vào mạng dùng riêng, có địa chỉ IP nguồn là địa chỉ IP của các máy tin cậy thì hệ thống tường lửa hay bộ lọc gói đều cho phép chúng đi qua. Phương pháp tấn công này được gọi là "giả địa chỉ IP" (IP spoofing). Nhờ phương pháp này, kẻ tấn công có thể đột nhập được vào các máy có đặt chế độ làm việc tin cậy và các máy khác trong mạng dùng riêng.

1.2.3. Giả điều khiển TCP (TCP spoofing)

Một kết nối TCP được định nghĩa đầy đủ với 4 tham số: địa chỉ IP nguồn, số hiệu cổng TCP nguồn, địa chỉ IP đích, số hiệu cổng TCP đích, Phần tiêu đề để gói IP chứa địa chỉ ICP nguồn, địa chỉ IP đích và phân loại giao thức vận chuyển (TCP=6). Phần tiêu đề để gói TCP có chứa số hiệu cổng nguồn, số hiệu cổng đích, các số tuần tự (sequence) và báo nhận (acknowledge) cũng như các cờ như: SYN, ACK, RST, FIN,.v.v… Khi một gói IP đi qua một giao diện mạng của hệ thống, ta có thể đọc được nội dung của gói đó, bao gồm các giá trị trả lời số tuần tự STN/ACK hiện thời của các gói trên kết nối đó.

Khi bắt được một gói, hệ thống của kẻ tấn công có thể tạo ra các gói số liệu IP giả có cùng địa chỉ IP nguồn, số hiệu cổng TCP nguồn cũng như các giá trị SEQ/ACK và các cờ của TCP đặt trong gói sao cho hệ thống đích bị đánh lừa, ngộ nhận gói số liệu thu được là gói số liệu của bên phát thật.

Đồng thời, hệ thống của kẻ tấn công còn gửi gói TCP cho hệ thống nguồn với cờ FIN = 1 (kết thúc kết nối) hay cờ RST = 1 (khởi tạo lại) để đánh lừa hệ thống đích muốn kết thúc kết nối với hệ thống nguồn. Sau khi bị lừa, bên phát kết thúc kết nối vời hệ thống nguồn, Sau khi bị lừa, bên phát kết thúc kết nối TCP với bên thu, trong khi bên thu lại tưởng hệ thống của kẻ tấn công là bên phát và tiếp tục trao đổi số liệu.

1.2.4. Session hijacking

Khi bên phát S và bên thu D thiết lập kết nối cũng như truyền số liệu, mối tin tưởng của S và D với nhau là: địa chỉ IP nguồn, địa chỉ TCP nguồn, địa chỉ IP đích, địa chỉ TCP đích và các giá trị SEQ/ACK.

Nếu kẻ tấn công (hacker) làm lẫn lộn các giá trị SEQ/ACK trong các gói từ S đến D thì D sẽ không còn tin tưởng các gói thật từ S đến nữa. Khi đó, kẻ tấn công sẽ giả làm S, dùng đúng các giá trị SEQ/ACK của S để tiếp tục trao đổi số liệu với D.

Phương thức tấn công loại này, nghĩa là làm lẫn lộn các giá trị SEQ/ACK từ S đến D, được thực hiện bằng cách chèn các gói số liệu vào đúng thời điểm gói từ S đến D, làm cho D chấp nhận gói số liệu lừa này và cập nhật giá trị ACK của nó.

1.2.5. Giả yêu cầu thiết lập kết nối

Bình thường, khi một máy trạm muốn thiết lập một liên kết TCP với máy phục vụ, nó gửi một gói TCP với cờ SYN = 1, yêu cầu thiết lập kết nối. Khi máy phục vụ nhận được gói SYN, nó xác nhận bằng cách gửi gói SYN/ACK (SYN= 1 và ACK = 1) cho máy trạm. Khi nhận được gói này, máy trạm cũng xác nhận lại bằng gói SYN/ACK và kết nối thiết lập. Quá trình thiết lập kết nối này được gọi là quá trình bắt tay 3 bước.

Khi sử dụng SYN để tấn công, gói SYN đầu tiên được gửi tới máy phục vụ đã bị giả địa chỉ IP nguồn, hoặc được thay thế bằng một địa chỉ IP không tồn tại, hoặc là địa chỉ IP của một máy tính khác.

Khi nhận được các gói đồng bộ SYN này, máy phục vụ sẽ cấp phát tài nguyên để xử lý và theo dõi các kết nối mới này và sau đó gửi lại các gói đồng bộ SYN/ACK. Rõ ràng, các gói SYN/ACK được gửi tới cho một địa chỉ giả hay địa chỉ IP đã bị lừa và vì vậy, máy phục vụ sẽ không nhận được các gói SYN/ACK (bước 3) từ phía máy trạm để thiết lập kết nối. Nó sẽ gửi lại vài gói SYN/ACK nữa (5 lần với Windows NT), đồng thời tăng giá trị time – out cho mỗi lần truyền lại (3, 6, 12, 24, 48s với Windows NT). Sau lần truyền lại gói SYN – ACK cuối cùng, máy phục vụ sẽ từ bỏ kết nối và giải phóng các tài nguyên đã cấp phát cho kết nối.

Như vậy, tổng số thời gian chiếm giữ tài nguyên cho TCP cho kết nối đó là lớn và “vô nghĩa” (với Windows NT khoảng 189 s). Với kiểu tấn công này, máy phục vụ

sẽ bị cạn kiệt tài nguyên TCP và không có khả năng xử lý tiếp tục các kết nối TCP mới nữa (SYN flood attack).

1.2.6. Tấn công phân đoạn IP

Các hệ định tuyến dễ bị tấn công bởi phương pháp này. Thông thường, các hệ định tuyến đều có các danh sách điều khiển truy nhập ACL (Access Control List).

Danh sách này được thiết lập bởi người quản trị mạng, cho phép tạo các luật lọc gói trong hệ định tuyến. Các gói IP có được qua hay không đều dựa vào danh sách điều khiển truy nhập ACL.

Bình thường, nếu phân đoạn IP đầu tiên được phép đi qua dựa trên ACL thì hệ định tuyến sẽ chuyển gói đi đúng đích. Sau đó, nó sẽ chuyển tuần tự các phân đoạn IP tiếp theo mà không kiểm tra dựa trên ACL nữa. Trong phương thức tấn công này, kẻ tấn công dùng các phân đoạn IP sau ghi đè lên phần cuối của phân đoạn đầu tiên, đánh lừa hệ định tuyến để chấp nhận gói thay vì phải từ chối (Overlapping Fragments or IP frags attack).

1.3. HIỂM HỌA ĐE DỌA DỊCH VỤ MẠNG MÁY TÍNH.

1.3.1. Hiểm họa dịch vụ thư điện tử.

Đối với dịch vụ thư điện tử SMTP, có một mối đe dọa sau đây:

Từ chối thư điện tử: Đây là mối đe dọa làm tê liệt máy phục vụ thư điện tử bằng cách gửi liên tiếp các bức thư điện tử có kích thước cực lớn, còn gọi là “bom thư”. Thông thường, các máy phục vụ thư không có khả năng nhận các bức thư lớn hơn 1MByte, hoặc nhận một số lượng lớn thư tại cùng một thời điểm,… Trong trường hợp này, máy phục vụ thư không có khả năng xử lý các truy nhập hộp thư một cách hợp pháp cũng như nhận và chuyển tiếp các gói thư có độ lớn thông thường khác.

Các tệp gắn kèm thư điện tử cũng là mối hiểm họa tiềm tàng đối với hệ thống và các dịch vụ thông tin. Người dùng thư điện tử chỉ cần mở tệp gắn kèm khi đọc thư là đủ để kích hoạt một chương trình (được giấu dưới dạng một tệp số liệu gắn kèm thư điện tử) thu thập thông tin về hệ thống, người sử dụng, số liệu ứng dụng hoặc lây

lan virus, phá hỏng hệ thống,… Các hiểm họa này đặc biệt nguy hiểm đối với môi trường và ngôn ngữ lập trình trên mạng như Java và ActiveX.

1.3.2. Hiểm họa đe dọa dịch vụ Web

Mối đe doa lớn nhất đối với dịch vụ Web là người dùng trái phép:

Thay đổi số liệu Web trên trang Web tương ứng; truy nhập vào hệ thống điều hành của máy phục vụ Web. Bằng việc viết và gửi các chương trình chuyên biệt kèm theo yêu cầu truy nhập số liệu Web hoặc bản thân số liệu Web, người dùng trái phép có thể gây ra tràn bộ đệm hoặc các trường hợp đặc biệt khác (Exception conditions) để chuyển hệ điều hành từ chế độ người dùng (user mode) sang chế độ hệ thống (system mode), và từ đó, dễ dàng thực hiện các hành đồng phá hoại như thay đổi nội dung trang Web, thay đổi cấu hình hệ thống, thay đổi chính sách quản trị hệ thống…

Biện pháp đơn giản nhất có thể thực hiện để chống lại mối đe dọa này là hạn chế quyền truy nhập và sử dụng các tài nguyên hệ thống của các phần mềm ứng dụng là phần mềm được thực hiện trong chế độ người dùng (user mode); kể cả các phần mềm được viết bằng Java script và các java applets. Ngoài ra, cũng có thể sử dụng các giao thức chuẩn để trao đổi số liệu Web được mã mật, ví dụ như: giao thức siêu văn bản mật SHTTP (Secure-HTTP), bộ giao thức vận chuyển mật SSL/TLS (Secure Socket layer/Transport Layer Security).

1.3.3. Hiểm họa dịch vụ Talnet

Mối đe dọa lớn nhất đối với dịch vụ Talnet là – theo quy định của chuẩn Talnet – tên người dùng hoặc/ và mật khẩu đăng nhập hệ thống không được bảo vệ, nghĩa là mã mật, khi truyền trên mạng – mỗi khi người dùng đăng nhập vào hệ thống (login process). Lúc này, nếu sử dụng bất kỳ một phần mềm giám sát thích hợp nào để thu tất cả số liệu trao đổi trên Talnet thì hoàn toàn có thể biết được rõ ràng tên hoặc/ và mật khẩu của người dùng.

Ngoài ra, bản thân chương trình Talnet có thể ghi lại rõ ràng tên và mật khẩu của người đăng ký sử dụng hệ thống, và vì vậy, một khi đã đăng nhập trái phép vào hệ thống thì hoàn toàn có thể đọc được tên và mật khẩu rõ ràng của người dùng cũng như các thông số hệ thống khác.

Cách đơn giản nhất để chống lại mối đe dọa dịch vụ Talnet này là mã mật nội dung số liệu trao đổi trên kết nối Talnet, bao gồm tên, mật khẩu người dùng và số liệu.

1.3.4. Hiểm họa dịch vụ FTP

Dịch vụ FTP thường bị đe dọa khi không được quản lý một cách chặt chẽ, nhất là các thư mục số liệu riêng, nội bộ không được lưu giữ mội cách *tách biệt* với các thư mục số liệu, "công cộng" để cung cấp dịch vụ FTP.

Trong những trường hợp này, người sử dụng dịch vụ FTP để truy nhập các số liệu công cộng có thể tải về các số liệu nội bộ, không công khai một cách hết sức dễ dàng. Hơn thế nữa, người dùng trái phép còn có thể thay đổi quyền truy nhập vào các tệp số liệu khác mà họ quan tâm để tải về được các số liệu này hoặc làm đảo lộn chính sách quản lý quyền truy nhập hệ thống và các ứng dụng được thiết lập trước đó.

Tương tự như dịch vụ Talnet, tên và mật khẩu của người dùng trong dịch vụ FTP cũng không được bảo vệ, và vì vậy, đây cũng là một mối đe dọa lớn; tên và mật khẩu người dùng rất dễ bị lộ nếu có người dùng trái phép thu và phân tích số liệu trên kết nối FTP, Ngoài ra, các địa chỉ FTP còn là các địa chỉ công khai "phổ biến" các phần mềm lậu, trái phép.

1.3.5. Các lỗ hổng trên mạng

1.3.5.1. Phân loại lỗ hổng theo mức độ

a/. Các lỗ hổng loại C

Các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS.

Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống mà không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.

Các dịch vụ có chứa đựng lỗ hổng cho phép thực hiện các cuộc tấn công DoS có thể được nâng cấp hoặc sửa chữa bằng các phiên bản mới hơn của các nhà cung cấp dịch vụ. Hiện nay, chưa có một giải pháp toàn diện nào để khắc phục các lỗ hổng loại này vì bản thân việc thiết kế giao thức ở tầng Internet (IP) nói riêng và bộ giao thức TCP/IP đã chứa đựng những nguy cơ tiềm tàng của các lỗ hổng này.

Một lỗ hổng loại C khác cũng thường thấy đó là các điểm yếu của dịch vụ cho phép thực hiện tấn công làm ngưng trệ hệ thống của người sử dụng cuối; Chủ yếu với hình thức tấn công này là sử dụng dịch vụ Web. Giả sử: trên một Web Server có những trang Web trong đó có chứa các đoạn mã Java hoặc JavaScripts, làm "treo" hệ thống của người sử dụng trình duyệt Web của Netscape bằng các bước sau:

- Viết các đoạn mã để nhận biết được Web Browers sử dụng Netscape.
- Nếu sử dụng Netscape, sẽ tạo một vòng lặp vô thời hạn, sinh ra vô số các cửa sổ, trong mỗi cửa sổ đó nối đến các Web Server khác nhau.

Với một hình thức tấn công đơn giản này, có thể làm treo hệ thống. Đây cùng là một hình thức tấn công kiểu DoS. Người sử dụng trong trường hợp này chỉ có thể khởi động lại hệ thống.

Một lỗ hổng loại C khác cũng thường gặp đối với các hệ thống mail là không xây dựng các cơ chế anti-relay (chống relay) cho phép thực hiện các hành động spam mail. Như chúng ta đã biết, cơ chế hoạt động của dịch vụ thư điện tử là lưu và chuyển tiếp. Một số hệ thống mail không có các xác thực khi người dùng gửi thư, dẫn đến tình trạng các đối tượng tấn công lợi dụng các máy chủ mail này để thực hiện spam mail. Spam mail là hành động nhằm tê liệt dịch vụ mail của hệ thống bằng cách gửi một số lượng lớn các tin tới một địa chỉ không xác định, vì máy chủ mail luôn phải tốn năng lực đi tìm những địa chỉ không có thực dẫn đến tình trạng ngưng trệ dịch vụ. Số lượng các tin có thể sinh ra từ các chương trình làm bom thư rất phổ biến trên mạng Internet.

b/. Các lỗ hổng loại B

Các lỗ hổng loại này cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần kiểm tra tính hợp lệ.

Mức độ nguy hiểm trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến mất hoặc lộ thông tin yêu cầu bảo mật.

Một số lỗ hổng loại B thường xuất hiện trong ứng dụng gửi mail :

- Gửi mail (sendmail) là một chương trình được sử dụng rất phổ biến trên hệ thống UNIX để thực hiện gửi thư điện tử cho những người sử dụng trong nội bộ

mạng. Thông thường, sendmail là một chương trình chạy ở chế độ nền được kích hoạt khi khởi động hệ thống. Trong trạng thái hoạt động, sendmail sẽ mở cổng 25 đợi một yêu cầu tới sẽ thực hiện gửi hoặc chuyển tiếp thư. Sendmail khi được kích hoạt sẽ chạy dưới quyền root hoặc quyền tương ứng. Lợi dụng đặc điểm này và một số lỗ hổng trong các đoạn mã của sendmail, kẻ tấn công có thể dùng sendmail để đạt được quyền root trên hệ thống.

- Để khắc phục lỗi của sendmail cần tham gia các nhóm tin về bảo mật. Vì sendmail là một chương trình có khá nhiều lỗi. Nhưng cũng có nhiều người sử dụng nên các lỗ hổng bảo mật thường được phát hiện và khắc phục nhanh chóng. Khi phát hiện lỗ hổng trong sendmail cần nâng cấp, thay thế phiên bản sendmail đang sử dụng.

Một loạt các vấn đề khác về quyền sử dụng chương trình trên UNIX cũng thường gây nên các lỗ hổng loại B.

Các lỗ hổng loại B khác :

- Những chương trình viết bằng C. Vì những chương trình này thường sử dụng một vùng đệm – là một vùng trong bộ nhớ sử dụng để lưu dữ liệu trước khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng với quy định trường này dài 20 ký tự. Họ sẽ khai báo :

```
char first_name [20];
```

Với khai báo này, cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu ở vùng đệm, nếu người sử dụng nhập hơn 25 ký tự, sẽ xảy ra hiện tượng tràn vùng đệm và kết quả là số ký tự dư thừa sẽ nằm ở một vị trí không kiểm soát được trong bộ nhớ.

Đối với những kẻ tấn công, chúng sẽ lợi dụng lỗ hổng này để nhập vào những ký tự đặc biệt, để thực thi một số lệnh đặc biệt trên hệ thống. Thông thường, lỗ hổng

này thường được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

c/. Các lỗ hổng loại A

Có mức độ rất nguy hiểm, đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Ví dụ các Web Server thường có một script mà khi chạy script đó, người sử dụng có thể nhìn thấy cũng như đọc được nội dung toàn bộ các file trong hệ thống.

Những lỗ hổng loại này hết sức nguy hiểm vì nó tồn tại sẵn có trên phần mềm sử dụng. Người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng sẽ có thể bỏ qua những điểm yếu này.

Đối với những hệ thống cũ, thường xuyên phải kiểm tra các thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này. Một loạt các chương trình phiên bản cũ thường sử dụng có các lỗ hổng loại A như: FTP, Gopher, Telnet, Sendmail, ARP, finger…

1.3.5.2. Lỗ hổng trong ứng dụng máy tính

a/. Lỗ hổng trong chương trình.

- **Lỗi tràn vùng đệm (Daemon finger)**

Một lỗ hổng của Daemon finger là cơ hội để phương thức tấn công Worm (Sâu) trên Internet phát triển. Đó là lỗi tràn vùng đệm trong các tiến trình (Lỗi khi lập trình).

Vùng đệm để lưu chuỗi ký tự nhập vào được giới hạn là 512 bytes. Tuy nhiên chương trình không thực hiện kiểm tra dữ liệu vào khi lớn hơn 512 bytes, trước khi nó được thi hành.

Kết quả là xảy ra hiện tượng tràn dữ liệu vùng đệm khi dữ liệu lớn hơn 512 bytes. Phần dữ liệu dư thừa sẽ kích hoạt một script khác hoạt động. Script này tiếp tục thực hiện tới một máy chủ khác. Dẫn đến hình thành một mắt xích các Worm trên mạng Internet.

- **Chương trình quét (Scanner)**

Scanner là chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm làm việc cục bộ, hay trên một trạm ở xa.

Những yếu tố để một chương trình Scanner có thể hoạt động là:

- Hệ thống có hỗ trợ TCP/IP.
- Hệ thống kết nối Internet.

- **Công nghệ Java trong bảo mật dịch vụ Web**

Ngôn ngữ lập trình Java được Sun xây dựng và phát triển. Một trong những điểm mạnh của Java là hỗ trợ bảo mật rất cao. Tuy nhiên vẫn có một số lỗ hổng được phát hiện:

- Trình duyệt Netscape 2.0 và 2.1 có một số lỗ hổng cho phép chạy các Java Applet có chức năng xóa các file trên hệ thống.
- Cho phép các cuộc tấn công DoS.
- Một số Applet cho phép tạo các kết nối tới địa chỉ tùy ý mà người dùng không kiểm soát được.

- **Một số lỗ hổng của JavaScript**

Không giống như các lỗ hổng bảo mật của Java, các lỗ hổng bảo mật của JavaScript thường liên quan đến thông tin người dùng:

- Netscape Communicator 4.4 có thể dùng các đoạn mã JavaScript đọc thông tin các tham số cài đặt hệ thống.
- Netscape Communicator đến phiên bản 4.5, cho phép chạy các đoạn mã JavaScript đọc nội dung các địa chỉ URL trong Cache.

b/. Lỗ hổng trong ứng dụng

- **File host.equiv**

Nếu một người dùng được xác định trong file host.equiv cùng với địa chỉ máy của họ, thì người này được phép truy nhập từ xa vào hệ thống đã khai báo.

Tuy nhiên khi thực hiện chức năng trên, nó cho phép người truy nhập từ xa có quyền của bất cứ người nào trên hệ thống => xuất hiện lỗ hổng.

Ví dụ: Trên máy A, file ect/host.equiv có dòng định danh B Julie, thì Julie trên B có thể truy nhập vào hệ thống trên A, và có được quyền của bất cứ người nào khác trên A.

- **Thư mục var/mail**

Nếu thư mục var/mail được thiết lập với quyền được ghi đối với mọi người trên hệ thống, thì bất cứ ai cũng có thể tạo file trong thư mục này.

Sau đó tạo một file đường dẫn với tên là tên của một người có trong hệ thống, đường dẫn tới một file trên hệ thống, thì các thư tới người dùng có tên trùng với tên file đường dẫn, sẽ được gán trong file mà nó trỏ tới.

Ví dụ: Một người dùng tạo đường dẫn từ var/mail/root tới /etc/password. Sau đó gửi mail bằng tên một người mới tới root, thì tên người dùng mới này sẽ được gán thêm vào trong file /etc/password.

- **Chức năng Proxy của FTPD**

FTPd là tiến trình máy chủ chuyển file qua Internet DARPA (Defense Advanced Research Projects Agency). Máy chủ sử dụng giao thức TCP và lắng nghe tại cổng đặc biệt trong đặc tả của dịch vụ FTP.

Chức năng Proxy của FTPd cho phép người dùng có thể truyền file từ một FTPd này tới một máy chủ FTPd khác. Sử dụng các chức năng này có thể bỏ qua các xác thực dựa trên địa chỉ IP.

Nguyên nhân là người dùng có thể yêu cầu một file trên máy chủ FTP, gửi file tới bất kỳ địa chỉ IP nào, trong file đó có các lệnh PORT và PASV tới các máy chủ, đang nghe trên các cổng TCP ở bất kỳ host nào.

Kết quả là một trong các host đó có máy chủ FTP đang chạy, và tin cậy người dùng đó, bỏ qua xác thực địa chỉ IP.

1.3.6. Ảnh hưởng của các lỗ hổng bảo mật trên mạng Internet

Những người tấn công có thể lợi dụng những lỗ hổng này để tạo ra những lỗ hổng khác tạo thành một chuỗi mắt xích những lỗ hổng. Ví dụ, một người muốn xâm nhập vào hệ thống mà anh ta không có tài khoản truy nhập hợp lệ trên hệ thống đó.

Trong trường hợp này, trước tiên anh ta sẽ tìm ra các điểm yếu trên hệ thống, hoặc từ các chính sách bảo mật, hoặc sử dụng các công cụ dò sét thông tin trên hệ thống đó để đạt được quyền truy nhập vào hệ thống. Sau khi mục tiêu như nhất đã đạt được, anh ta có thể tiếp tục tìm hiểu các dịch vụ trên hệ thống, nắm bắt được các điểm yếu và thực hiện các hành động tấn công tinh vi hơn.

Tuy nhiên, có phải bất kỳ lỗ hổng bảo mật nào cùng nguy hiểm đến hệ thống hay không? Có rất nhiều thông báo liên quan đến lỗ hổng bảo mật trên mạng Internet, hầu hết trong số đó là các lỗ hổng loại C, và không đặc biệt nguy hiểm đối với hệ thống. Ví dụ, khi những lỗ hổng về sendmail được thông báo trên mạng, không phải ngay lập tức ảnh hưởng trên toàn bộ hệ thống. Khi những thông báo về lỗ hổng được khẳng định chắc chắn, các nhóm tin sẽ đưa ra một số phương pháp để khắc phục hệ thống.

Trên mạng Internet có một số nhóm tin thường thảo luận về các chủ đề liên quan đến các lỗ hổng bảo mật đó là:

+ CERT (Computer Emergency Reponse Team): Nhóm tin này hình thành sau khi có phương thức tấn công Worm xuất hiện trên mạng Internet. Nhóm tin này thường thông báo và đưa ra các trợ giúp liên quan đến các lỗ hổng bảo mật. Ngoài ra nhóm tin còn có những báo cáo thường niên để khuyến nghị người quản trị mạng về các vấn đề liên quan đến bảo mật hệ thống. Địa chỉ Web site của nhóm tin: http://www.cert.org/

+ CIAC (Department of Energy Computer Incident Advisory Capability): tổ chức này xây dựng một cơ sở dữ liệu liên quan đến bảo mật cho bộ năng lượng của Mỹ. Thông tin của CIAC được đánh giá là một kho dữ liệu đầy đủ nhất về các vấn đề liên quan đến bảo mật hệ thống. Địa chỉ web site của CIAC :http://ciac.llnl.org/

+ FIRST (The Forum of Incident Response and Security Teams): Đây là một diễn đàn liên kết nhiều tổ chức xã hội và tư nhân, làm việc tình nguyện để giải quyết

các vấn đề về an ninh của mạng Internet. Địa chỉ Web site của FIRST:http://www.first.org./ Một số thành viên của FIRST gồm:

- CIAC
- NASA Automated Systems Incident Response Capability.
- Purdue University Computer Emergency Response Team
- Stanford University Security Team
- IBM Emergency Response Team

Chương 2: MỘT SỐ PHƯƠNG PHÁP BẢO VỆ THÔNG TIN TRÊN MẠNG MÁY TÍNH.

2.1. KIỂM SOÁT VÀ XỬ LÝ CÁC DẠNG TẤN CÔNG MẠNG.

Dựa vào những "Lỗ hổng" thiếu an ninh trên mạng máy tính: Những "Lỗ hổng" này có thể là điểm yếu của dịch vụ mà Hệ thống cung cấp.

Sử dụng các công cụ để phá hoại mạng máy tính: Ví dụ sử dụng các chương trình phá mật khẩu để truy nhập bất hợp pháp vào mạng máy tính.

Kết hợp cả hai hình thức trên để tấn công mạng máy tính.

8 phương pháp tấn công mạng máy tính phổ biến:

2.1.1. Tấn công giả mạo: Spoofing

Các hệ thống mạng trong doanh nghiệp ngày này thường xuyên phải đối mặt với rất nhiều kiểu tấn công từ bên ngoài cũng như bên trong. Một trong những cách tấn công mạng là dùng phương pháp giả mạo địa chỉ IP (IP spoofing), giả mạo DNS… Dưới đây là giới thiệu về phương pháp giả mạo địa chỉ IP.

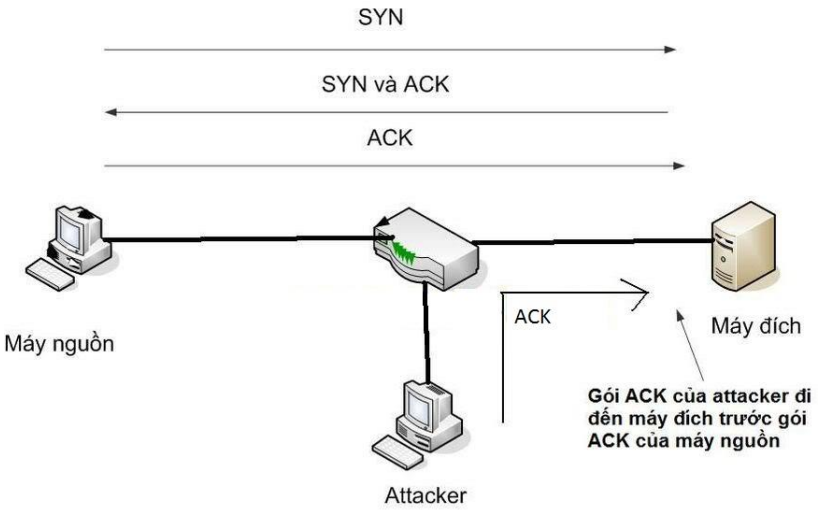
Ý tưởng cơ bản đầu tiên là máy của kẻ tấn công (attacker) sẽ tự biến mình thành một máy tin cậy:

- Nếu kẻ tấn công thuyết phục được một máy khác rằng nó là một máy khách tin cậy, thì từ đó có thể chiếm quyền tuy nhập máy chủ đó. Máy tấn công cũng có thể lấy được tài khoản và mật khẩu.

- Bạn có thể bị xem là đồng phạm của các cuộc tấn công. Lý do là thủ phạm thực sự có thể sử dụng IP giả mạo và IP giả mạo này vô tình trùng với IP của chính bạn.

Để hiểu tấn công giả mạo IP là một cách tấn công khả thi, ta sẽ xem xét hoạt động của IP và TCP. Tại lớp mạng (network) trong mô hình OSI, máy tấn công có thể dễ dàng chỉnh sửa gói tin của mình, thay đổi IP nguồn trong gói tin đó trở thành một IP tin cậy. Tuy nhiên, với TCP, hoạt động ở tầng giao vận có thể có nhiều khó khăn hơn.

Chúng ta đã biết trong phần đầu của những gói dữ liệu luôn có địa chỉ IP của nguồn xuất phát dữ liệu và chỉ số thứ tự (sequence number – dùng để sắp xếp các gói dữ liệu nhận được theo một thứ tự định sẵn). Để có thể lấy quyền điều khiển một phiên làm việc đang thiết lập giữa nguồn hợp pháp và host đích, kẻ tấn công cần biết về số thứ tự đó. Nếu kẻ tấn công dự đoán đúng số thứ tự, hắn có thể gửi tới host đích một gói tin ACK chính xác. Khi đó, chỉ cần gói tin ACK của kẻ tấn công tới được đích trước gói tin ACK gốc, thì kẻ tấn công sẽ được tin cậy bởi host đích:



Hình 2-1: Tấn công Spoofing

Làm thế nào kẻ tấn công có thể biết chính xác số TCP sequence dựa trên cách giả mạo địa chỉ IP được sử dụng? Ta có 2 loại giả mạo địa chỉ IP, với mỗi loại như vậy thì kẻ tấn công có kỹ thuật tấn công khác nhau:

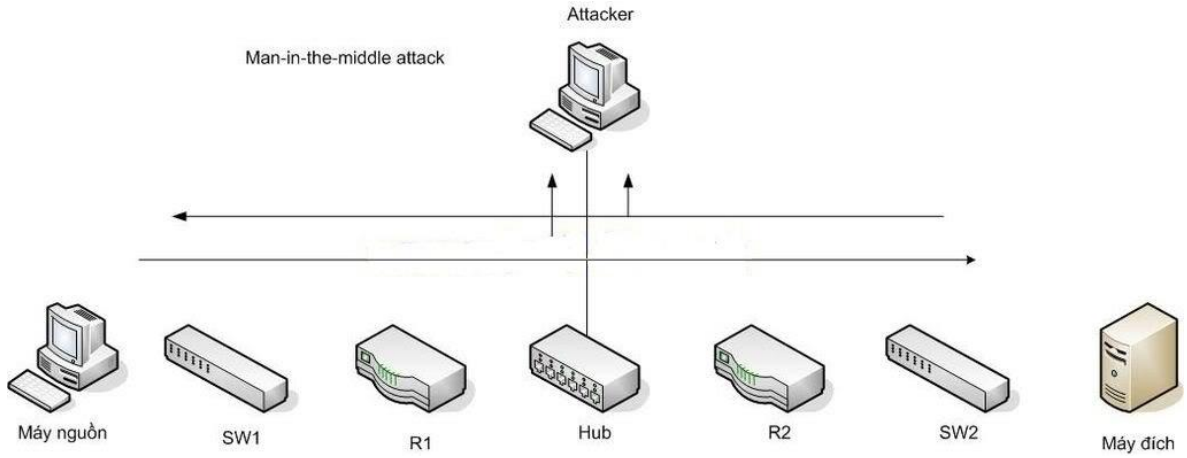
- Giả mạo bằng cách bắt gói tin: Diễn ra khi máy tấn công và mục tiêu ở trên cùng một subnet. Khi đó, kẻ tấn công có thể sử dụng công cụ bắt gói tin, phân tích gói tin để có thể có được số thứ tự.

- Giả mạo địa chỉ IP từ xa: Diễn ra khi máy tấn công khác subnet với mục tiêu. Khi đó, việc có được số TCP sequence chính xác là rất khó. Tuy nhiên, với một số kỹ thuật, chẳng hạn như định tuyến theo địa chỉ nguồn (IP source routing), máy tấn công cũng có thể xác định chính xác được chỉ số đó.

Tấn công giả mạo địa chỉ IP cục bộ bằng kỹ thuật tấn công Man-in-the-middle là phương pháp được sử dụng khi máy tấn công có cùng subnet với máy nạn nhân, hắn có thể sử dụng cách tấn công này.

- Một trong những cách tấn công Man-in-the-middle là kẻ tấn công sẽ làm cách nào đó để hệ thống gửi frame qua máy của mình. Chẳng hạn, kẻ tấn công có thể gửi hàng loạt những gói tin ARP vu vơ tới hệ thống, những gói tin ARP đó có thể thông báo rằng địa chỉ MAC của kẻ tấn công là địa chỉ MAC của router kế tiếp. Do đó kẻ tấn công sẽ nhận được đường đi, rồi sau đó chuyển đường đi đến router kế tiếp thật sự. Và kết quả, người dùng đầu cuối không hề biết đường đi của mình đều đi qua một máy khác trong cùng mạng.

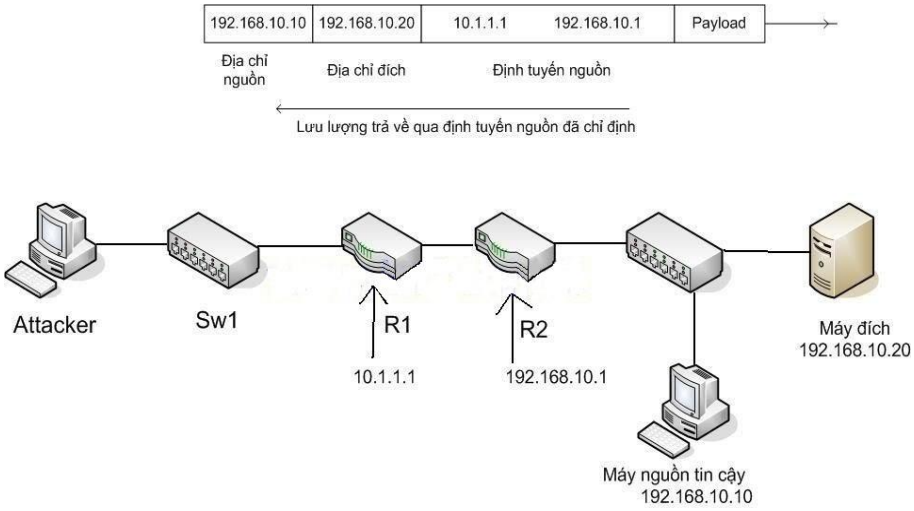
- Một dạng khác của việc tấn công Man-in-the-middle là khi kẻ tấn công nối Hub đến một vùng mạng có đường đi mà kẻ tấn công muốn có (hình dưới). Kẻ tấn công có thể sử dụng một công cụ bắt gói tin và phân tích để bắt lưu lượng đang di chuyển giữa hệ thống đầu cuối. Nếu gói tin bắt được là dạng text thông thường, kẻ tấn công hoàn toàn có thể thu được những thông tin nhạy cảm, chẳng hạn như thông tin người dùng và mật khẩu.



Hình 2-2: Tấn công Man-in-the-middle

IP source routing là một cơ chế cho phép một máy nguồn chỉ ra đường đi một cách cụ thể và không phụ thuộc vào bảng định tuyến của các router.

Nếu kẻ tấn công dùng kỹ thuật IP source routing, hắn có thể nhắm tới một đường định tuyến thành công đã có sẵn. Máy tấn công lúc này có thể gửi một gói tin IP với địa chỉ nguồn tự tạo trong IP header. Và khi host đích nhận được gói tin này, nó sẽ gửi đường đi ngược lại tới địa chỉ IP giả mạo thông qua đường định tuyến mà kẻ tấn công muốn. Cách tiếp cận này có thể vượt qua những khó khăn khi thực hiện việc tấn công giả mạo địa chỉ IP từ xa.



Hình 2-3: Tấn công giả mạo IP

Vậy nên để tránh những hiểm họa như vậy, hầu hết các hệ thống mạng đều tắt chức năng định tuyến theo nguồn.

Cách chống lại việc tấn công giả mạo địa chỉ IP:

- Dùng danh sách kiểm tra truy nhập (Access Control List – ACL).
- Dùng mật mã xác thực.
- Mã hóa đường truyền giữa các thiết bị.

2.1.2. Đánh hơi: Sniffing

Đánh hơi thường sử dụng các công cụ là Sniffer(2). Sniffer đơn giản được hiểu là một chương trình cố gắng lăng nghe các lưu lượng thông tin trong cùng một hệ thống mạng. Tương tự như các thiết bị cho phép nghe lén trên đường dây điện thoại.

Tuy nhiên, những giao dịch giữa các hệ thống mạng máy tính thường là những dữ liệu ở dạng nhị phân, vì vậy các chương trình Sniffer phải có tính năng phân tích

các giao thức (Protocol Analysis), cũng như tính năng giải mã (Decode) các dữ liệu ở dạng nhị phân sang dạng khác để hiểu được chúng. Do trong một hệ thống mạng, thường sử dụng những giao thức kết nối chung và đồng bộ, nên có thể sử dụng Sniffer ở bất cứ máy nào trong hệ thống.

Những đối tượng hay bị Đánh hơi (Sniffing) là:

- Password (từ Email, Web, SMB, FTP, SQL, Telnet).
- Các thông tin về thẻ tín dụng.
- Văn bản của Email.
- Các tệp tin đang được truyền trên mạng.

Sniffing thường được sử dụng vào 2 mục đích khác biệt nhau. Vừa là công cụ giúp cho các quản trị mạng theo dõi và bảo trì hệ thống mạng, vừa là một chương trình được cài vào một hệ thống với mục đích đánh hơi, nghe lén các thông tin trên mạng này. Dưới đây là một số tính năng của Sniffing được sử dụng theo cả hai hướng tích cực và tiêu cực:

- Tự động chụp các tên người sử dụng và mật khẩu không được mã hóa (Tính năng này thường được các kẻ tấn công sử dụng để tấn công hệ thống).
- Chuyển đổi dữ liệu trên đường truyền để những quản trị viên có thể đọc và hiểu được ý nghĩa của những dữ liệu đó.
- Nhìn vào lưu lượng của hệ thống cho phép các quản trị viên có thể phân tích những lỗi đang mắc phải trên hệ thống lưu lượng của mạng.
- Một số Sniffer hiện đại, còn có thêm tính năng tự động phát hiện và cảnh báo các cuộc tấn công đang được thực hiện vào hệ thống mạng.
- Ghi lại thông tin về các gói dữ liệu, các phiên truyền dữ liệu… Tương tự như hộp đen của máy bay, giúp các quản trị viên có thể xem lại thông tin về các gói dữ liệu, các phiên truyền sau các sự cố để phục vụ cho công việc phân tích, khắc phục các sự cố trên hệ thống mạng.

Các giao thức có thể sử dụng Sniffing:

- Telnet: Ghi lại các thông tin như thông tin đăng nhập, mật khẩu.
- HTTP: Các dữ liệu gửi đi mà không mã hóa.
- SMTP: Mật khẩu và các dữ liệu gửi đi mà không mã hóa.

- NNTP: Mật khẩu và các dữ liệu gửi đi mà không mã hóa.

- POP: Mật khẩu và các dữ liệu gửi đi mà không mã hóa.

- FTP: Mật khẩu và các dữ liệu gửi đi mà không mã hóa.

- IMAP: Mật khẩu và các dữ liệu gửi đi mà không mã hóa.

Phương thức hoạt động:

- Chủ động: Là Sniffing qua Switch, nó rất khó thực hiện và dễ bị phát hiện. Kẻ tấn công thực hiện loại tấn công này theo các bước như sau:

- Kẻ tấn công kết nối tới Switch bằng cách gửi địa chỉ MAC nặc danh.
- Switch xem địa chỉ kết hợp với mỗi khung (frame).
- Máy tính trong LAN gửi giữ liệu tới cổng kết nối.

- Bị động: Đây là loại Sniffing lấy dữ liệu qua Hub. Nó được gọi là bị động vì rất khó có thể phát hiện ra loại Sniffing này. Kẻ tấn công sẽ sử dụng máy tính của mình kết nối đến Hub và bắt đầu đánh hơi.

Các kiểu tấn công:

- ARP Poisoning.

- DNS Poisoning.

- Cướp phiên làm việc.

Phòng chống tấn công Sniffing:

- Mã hóa đường truyền.

- Tạo mục bảng ARP tĩnh cho các thiết bị trong mạng.

- Quản lý port console trên Switch.

- Bảo vệ các cổng.

- IDS và IPS.

- Phương pháp Ping.

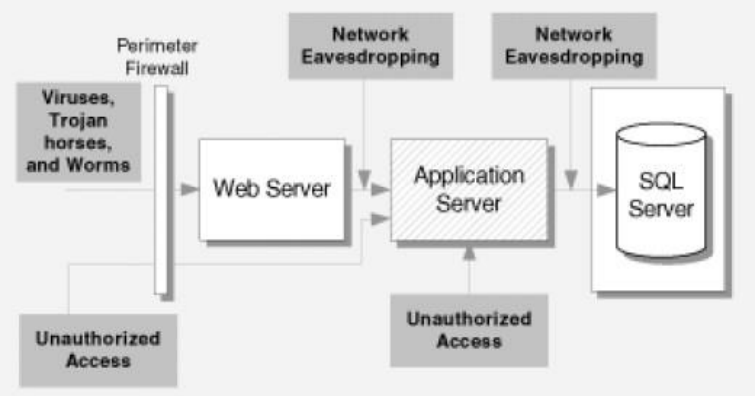
- Phương pháp ARP.

- Phương pháp sử dụng DNS.

- Phương pháp Định tuyến nguồn (Source Route).

- Phương pháp giăng bẫy.

2.1.3. Nghe lén: Mapping



Hình 2-4 : Tấn công Mapping

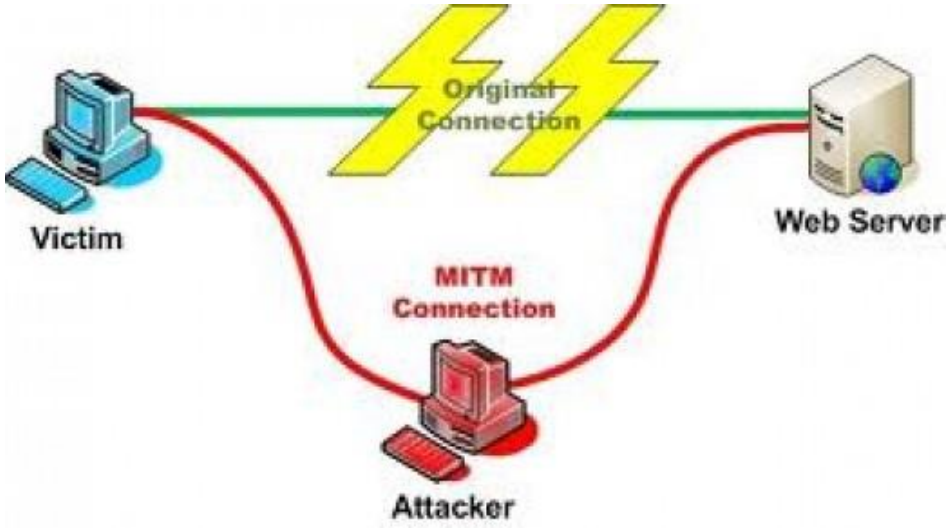
Trước khi tấn công vào một mạng, kẻ tấn công sẽ muốn biết được địa chỉ IP của các máy ở trong mạng, hệ điều hành họ sử dụng cũng như những dịch vụ họ đang sử dụng. Với những thông tin này, cuộc tấn công có thể tập trung hơn và có bị phát hiện hơn. Quá trình lấy thông tin như vậy được gọi là Mapping (Nghe lén).

Nhìn chung, tất cả các thông tin liên lạc trong mạng thường được gửi qua một văn bản có định dạng rõ ràng (Clear text) và không được bảo vệ, điều này cho phép kẻ tấn công đã đạt được quyền truy nhập vào đường dẫn dữ liệu trong mạng của bạn có thể lắng nghe hoặc phân tích được các đường dẫn. Khi kẻ tấn công nghe trộm được thông tin liên lạc của bạn, nó được gọi là đánh hơi (sniffing – đã được trình bày bên trên). Phòng trống nghe trộm là một vấn đề lớn nhất mà các quản trị viên phải đối mặt trong các doanh nghiệp.

2.1.4. Kiểu tấn công "Người đứng giữa": Hijacking

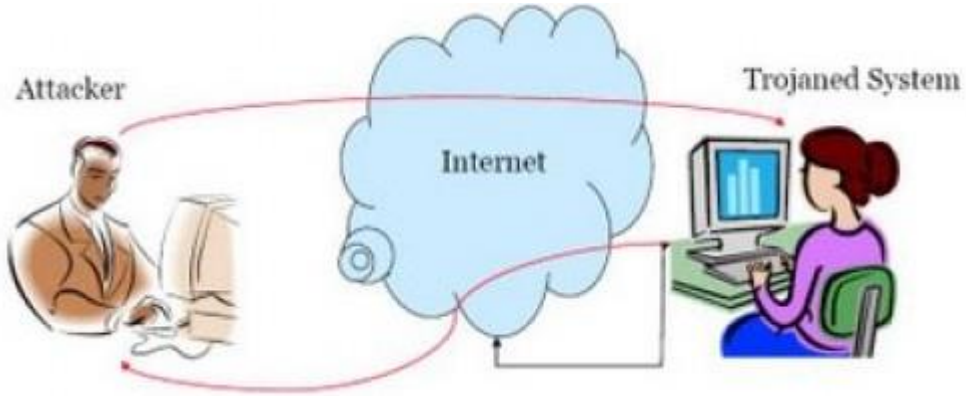
Đây là một kỹ thuật để tận dụng những điểm yếu trong giao thức TCP/IP. Tấn công xảy ra khi một người nào đó ở giữa bạn và máy chủ đang tích cực theo dõi, nắm bắt và kiểm soát thông tin của bạn.

Các cuộc tấn công này giống như một người nào đó giả danh tính của bạn để đọc tin nhắn của bạn. Kẻ tấn công đã cướp lấy phiên làm việc của bạn, giả danh là bạn và máy chủ sẽ tin rằng đó là bạn, vì kẻ tấn công sẽ tích cực trả lời như bạn, để giữ được việc trao đổi và có được nhiều thông tin. Trong khi đó, bạn sẽ tưởng rằng kết nối của mình tới máy chủ bị lỗi.



Hình 2-5 : Tấn công Hijacking

2.1.5. Ngựa thành Trojan: Trojans



Hình 2-6 : Tấn công Trojans

Trojans là loại phần mềm ác tính, không có khả năng tự sao chép nhưng có chức năng hủy hoại tương tự virus. Một trong những cách trojans giăng bẫy là nó tự nhận là giúp cho máy tính chống lại các virus nhưng thay vì làm vậy, nó quay ra đem virus vào máy.

Trojans được xuất phát từ điển tích Con ngựa thành Trojans trong thần thoại Hy Lạp.

Trojan horse là chương trình máy tính thường ẩn mình dưới dạng một chương trình hữu ích và có những chức năng mong muốn, hay ít nhất chúng trông như có các tính năng này. Một cách bí mật, nó lại tiến hành các thao tác khác không mong muốn. Những chức năng mong muốn chỉ là phần bề mặt giả tạo nhằm che giấu cho các thao tác này.

Trong thực tế, nhiều Trojan horse chứa đựng các phần mềm gián điệp nhằm cho phép máy tính thân chủ bị điều khiển từ xa qua hệ thống mạng.

Khác nhau căn bản với virus máy tính là Trojan Horse về mặt kỹ thuật chỉ là một phần mềm thông thường và không có ý nghĩa tự lan truyền. Các chương trình này chỉ lừa người dùng để tiến hành các thao tác khác mà thân chủ sẽ không tự nguyện cho phép tiến hành. Ngày nay, các Trojan horse đã được thêm vào đó các chức năng tự phân tán. Điều này đẩy khái niện Trojan horse đến gần với khái niệm virus và chúng trở thành khó phân biệt.

Một số thủ thuật tấn công :

- Trên các máy Microsoft Windows, người tấn công có thể đính kèm một Trojan horse vào một cái tên có vẻ lương thiện vào trong một thư điện tử với việc khuyến dụ người đọc mở đính kèm ra. Trojan horse thường là các tệp khả thi trên Windows và do đó sẽ có các đuôi như là .exe, .com, .scr, .bat, hay .pif. Trong nhiều ứng dụng của Windows đã có cấu hình mặc định không cho phép hiển thị các đuôi này. Do đó, nếu một Trojan horse có tên chẳng hạn là "Readme.txt.exe" thì tệp này sẽ hiển thị một cách mặc định thành "Readme.txt" và nó sẽ đánh lừa người dùng rằng đây chỉ là một loại hồ sơ văn bản không thể gây hại.

- Các biểu tượng cũng có thể được gán với các loại tệp khác nhau và có thể được đính kèm vào thư điện tử. Khi người dùng mở các biểu tượng này thì các Trojan horse ẩn giấu sẽ tiến hành những tác hại bất ngờ. Hiện nay, các Trojan horse không chỉ xoá các tệp, bí mật điều chỉnh cấu hình của máy tính bị nhiễm mà còn dùng máy này như là một cơ sở để tấn công các máy khác trong mạng.

- Lợi dụng một số lỗi của trình duyệt web, chẳng hạn như Internet Explorer, để nhúng Trojan vào một trang web, khi người dùng xem trang này sẽ bị nhiễm. Người dùng nên cập nhật các bản vá lỗi thường xuyên và dùng một trình duyệt web có độ bảo mật cao như Firefox và Google Chrome.

Các kiểu gây hại điển hình:

- Xóa hay viết lại các dữ liệu trên máy tính.
- Làm hỏng chức năng của các tệp.
- Lây nhiễm các phần mềm ác tính khác như virus.

- Cài đặt mạng để máy có thể bị điều khiển bởi máy khác.
- Đọc lén các thông tin cần thiết và gửi báo cáo đến nơi khác.
- Ăn cắp thông tin như là mật khẩu, số thẻ tín dụng…
- Đọc các chi tiết tài khoản ngân hàng và dùng vào các mục tiêu phạm tội.
- Cài đặt lén các phần mềm chưa được cho phép.

Cách phòng chống hữu hiệu nhất là đừng bao giờ mở các tệp đính kèm được gửi đến một cách bất ngờ. khi các đính kèm không được mở ra thì Trojans cũng không thể hoạt động. Các tệp tải về từ các dịch vụ chia sẻ tệp như là Kazaa hay Gnutella rất đáng nghi ngờ, vì các dịch vụ này thường bị dùng như là chỗ để lan truyền Trojans.

2.1.6. Tấn công từ chối dịch vụ: DoS

DoS cùng với DDoS là một trong những dạng tấn công nguy hiểm nhất đối với một hệ thống mạng.

Tấn công DoS là một kiểu tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng sẽ cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường đó là tấn công Denial of Service (DoS).

Mặc dù tấn công DoS không có khả năng truy nhập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp. Như định nghĩa trên, khi DoS tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công.

Mục đích của tấn công DoS :

- Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập, khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường.
- Cố gắng làm ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy nhập vào dịch vụ.
- Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó.

- Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy nhập vào.

- Khi tấn công DoS xảy ra, người dùng có cảm giác khi truy nhập vào dịch vụ đó như bị:

- Tắt mạng: Disable Network.
- Tổ chức không hoạt động: Disable Organization.
- Tài chính bị mất: Financial Loss.

Các dạng tấn công DoS:

- Tấn công Smurf: Là thủ phạm sinh ra cực nhiều giao tiếp ICMP (Ping) tới địa chỉ Broadcast của nhiều mạng với địa chỉ nguồn là mục tiêu cần tấn công.

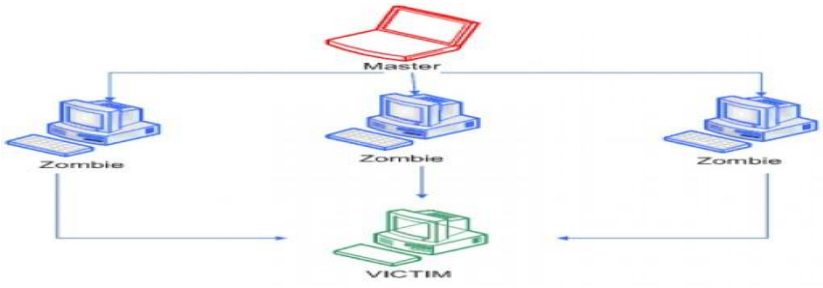
- Tấn công Buffer Overflow: Buffer Overflow xảy ra tại bất kỳ thời điểm nào đó có chương trình ghi lượng thông tin lớn hơn dung lượng của bộ nhớ đệm trong bộ nhớ.

- Tấn công Ping of Death: Kẻ tấn công gửi những gói tin IP lớn hơn số lượng bytes cho phép của tin IP là 65.536 bytes.

- Tấn công Teardrop: Gói tin IP rất lớn khi đến Router sẽ bị chia nhỏ làm nhiều phần nhỏ.

- Tấn công SYN flood: Kẻ tấn công gửi các yêu cầu ảo TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này, hệ thống cần tốn một lượng bộ nhớ cho kết nối.

2.1.7. Tấn công từ chối dịch vụ phân tán: DDoS



Hình 2-7: Tấn công DDoS

Tấn công từ chối dịch vụ phân tán (DDoS – Distributed Denial Of Service) là kiểu tấn công làm cho hệ thống máy tính hay hệ thống mạng quá tải, không thể cung

cấp dịch vụ hoặc phải dừng hoạt động. Trong các cuộc tấn công DDoS, máy chủ dịch vụ sẽ bị "ngập" bởi hàng loạt các lệnh truy cập từ lượng kết nối khổng lồ. Khi số lệnh truy cập quá lớn, máy chủ sẽ quá tải và không còn khả năng xử lý các yêu cầu. Hậu quả là người dùng không thể truy cập vào các dịch vụ trên các trang web bị tấn công DDoS.

Các kiểu tấn công DDoS:

- Những kiểu tấn công làm cạn kiệt băng thông của mạng:

o Flood Attack: Điều khiển các máy con (Zombie) gửi một lượng lớn yêu cầu đến hệ thống dịch vụ của mục tiêu, làm dịch vụ này bị hết khả năng về băng thông. Có 2 loại Flood Attack:

- UDP Flood Attack: UDP có tính chất kết nối yếu, hệ thống nhận tin của UDP chỉ đơn giản nhận vào tất cả các gói mình cần phải xử lý. Một lượng lớn các gói UDP được gửi đến hệ thống dịch vụ của mục tiêu sẽ đẩy toàn bộ hệ thống đến ngướng tới hạn.
- ICMP Flood Attack: Được thiết kế nhằm mục đích quản lý mạng cũng như định vị thiết bị mạng. Khi các Zombie gửi mộ tl]ơngj lớn ICMP_ECHO_REPLY đến mục tiêu thì hệ thống sẽ phải trả lời một lượng tương ứng các gói tin để trả lời, sẽ dẫn đến nghẽn đường truyền.

o Amplification Attack: Điều khiển các Zombie tự gửi tin nhắn đến một địa chỉ IP, làm cho tất cả các máy trong subnet này gửi tin nhắn đến hệ thống dịch vụ của mục tiêu, làm suy giảm băng thông của mục tiêu. Có hai loại Amplification Attack:

- Smurf Attack: Kẻ tấn công gửi gói tin đến bộ định tuyến, với địa chỉ của nạn nhân và bộ định tuyến sẽ gửi gói tin trả lời về địa chỉ IP của nạn nhân.
- Fraggle Attack: Tương tự Smurf Attack nhưng nguy hiểm hơn rất nhiều vì kẻ tấn công sẽ tạo ra một vòng lặp vô hạn việc gửi các gói tin từ bộ định tuyến về nạn nhân, từ nạn nhân tới bộ định tuyến.

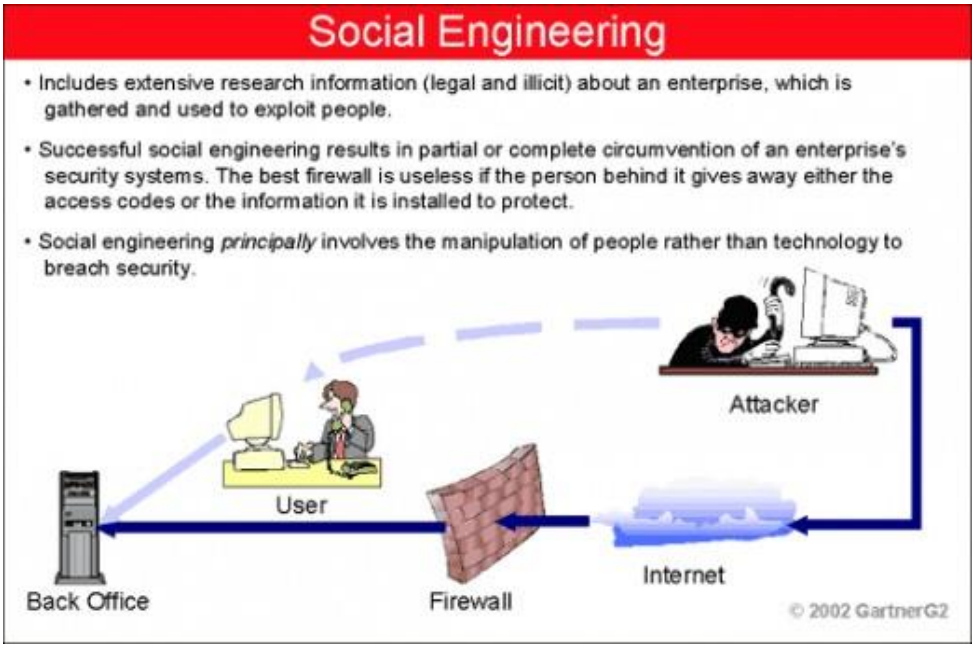
- Những kiểu tấn công làm cạn kiệt tài nguyên:

o Protocol Exploit Attack: Kẻ tấn công gửi một gói tin SYN đến nạn nhân với địa chỉ bên gửi là giả mạo, kết quả là sau khi nạn nhân gửi gói tin trả lời SYN/ACK và sẽ không bao giờ nhận được gói tin ACK cuối cùng, cho đến khi hết thời gian chờ,

nạn nhân mới nhận ra và giải phóng tài nguyên. Tuy nhiên, nếu lượng gói tin SYN giả mạo đến với số lượng nhiều, hệ thống có thể bị hết tài nguyên.

o Malformed Packet Attack: Dùng các Zombie để gửi các gói tin có cấu trúc không đúng chuẩn, làm cho hệ thống của nạn nhân bị treo.

2.1.8. Tấn công dựa trên yếu tố con người: Social engineering



Hình 2-8: Tấn công Social engineering

Là việc sử dụng lòng tin hay lừa dối để được truy cập vào hệ thống thông tin. Các cách thông dụng được sử dụng là qua điện thoại hoặc một tin nhắn từ Email. Kẻ tấn công thường xuyên giả vờ là quản lý trong một công ty đang đi công tác với một hạn nhất định để nhận những dữ liệu quan trọng trên hệ thống. Mục đích chính đằng sau kỹ thuật tấn công bằng yếu tố con người là đặt yếu tố con người trong vòng lặp mạng phi pháp và sử dụng như một vũ khí. Yếu tố con người sẽ trở thành điểm yếu lớn nhất trong an ninh mạng.

Các cách tấn công dựa trên yếu tố con người:

- Email giả mạo: Kẻ tấn công gửi một tin nhắn cho một hoặc nhiều người dùng trong một mạng rằng "Đây là quản lý hệ thống và mật khẩu của bạn phải được cài đặt

lại là 123” trong một khoảng thời gian tạm thời. Kẻ tấn công sẽ liên tục giám sát sự thay đổi và sau đó khai thác toàn bộ hệ thống.

- Cạnh tranh hư cấu: Kẻ tấn công sẽ thao túng một nhóm người dùng tham gia một vài cuộc cạnh tranh hư cấu cho một giải thưởng, với mục đích cuối cùng là khai thác được thông tin về an ninh mạng.

- Bàn trợ giúp hữu ích: Bàn trợ giúp nhận được một cuộc gọi từ kẻ tấn công thông báo rằng một người dùng đã quên mật khẩu, và người trợ giúp sẽ thông báo mật khẩu của người dùng được thay đổi thông qua điện thoại. Bây giờ, kẻ tấn công có tên người dùng và mật khẩu để làm việc.

2.2. DÙNG TƯỜNG LỬA.

2.2.1. Khái niệm tường lửa?

Tường lửa bảo vệ người sử dụng chống lại những kẻ tấn công từ bên ngoài bằng cách chặn các mã nguy hiểm hoặc lưu lượng Internet không cần thiết vào máy tính hay mạng của người sử dụng. Tường lửa có thế được cấu hình để khóa dữ liệu từ các vị trí cụ thể trong khi vẫn đảm bảo cho dữ liệu cần thiết có thể đi qua. Chúng thực sự quan trọng đối với những người thường xuyên kết nối Internet. Như vậy có thể nói việc tìm hiểu và nghiên cứu về công nghệ tường lửa đã và đang trở thành một vấn đề cấp thiết, đặc biệt là đối với những người chuyên sâu về lĩnh vực bảo mật. Các hình thức tấn công qua mạng Internet cũng như biện pháp chung để bảo vệ, ngăn chặn những cuộc tấn công đó. Và đi sâu vào nghiên cứu một loại thiết bị bảo vệ mạng khỏi thế giới bên ngoài đó là tường lửa.

Thuật ngữ tường lửa có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hoả hoạn. Trong công nghệ mạng thông tin, tường lửa 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 của một số thông tin khác không mong muốn.

Tường lửa Internet là một tập hợp thiết bị (bao gồm phần cứng và phần mềm) được đặt giữa mạng nội bộ (Intranet) của một tổ chức, một công ty, hay một quốc gia và Internet. Trong một số trường hợp, tường lửa có thể được thiết lập ở trong cùng một mạng nội bộ và cô lập các miền an toàn.

"***Tường lửa***" trong công nghệ mạng thông tin được hiểu là một hệ thống gồm phần cứng, phần mềm hay hỗn hợp phần cứng – phần mềm, có tác dụng như một ***tấm ngăn cách*** giữa các tài nguyên thông tin của mạng nội bộ với thế giới Inrernet bên ngoài.

Phạm vi hẹp hơn như trong một mạng nội bộ, người ta cũng bố trí "***Tường lửa***" để ngăn cách các miền an toàn khác nhau (Security Domain).

Kỹ thuật này phục vụ cho An toàn Hệ thống máy tính là chính, nhưng cũng hỗ trợ đảm bảo An toàn truyền tin, ví dụ chống trộm cắp, sửa đổi thông tin (chẳng hạn làm sai lệch tin tức hay giả mạo chữ ký) trước khi đến tay người nhận.

2.2.2. Ứng dụng của tường lửa

2.2.2.1. Tường lửa bảo vệ cái gì?

Dữ liệu, tài nguyên và thông tin cá nhân của tổ chức cũng như người sử dụng là những đối tượng cần được bảo vệ. Nếu máy tính không được bảo vệ, khi kết nối Internet, tất cả các giao thức ra vào mạng đều được cho phép, vì thế tin tặc, Trojan, virus có thể truy cập và lấy cắp thông tin cá nhân của người sử dụng trên máy tính.

Chúng có thể cài đặt các đoạn mã để tấn công tập tin trên máy tính. Chúng có thể sử dụng máy tính của người sử dụng đề tấn công một máy tính của gia đình hoặc doanh nghiệp khác kết nối Internet. Một tường lửa có thể giúp người sử dụng thoát khỏi gói tin hiểm độc trước khi nó đến hệ thống của người sử dụng.

2.2.2.2. Tường lửa chống lại cái gì?

Tường lửa bảo vệ hệ thống của người sử dụng chống lại các loại tấn công. Dưới đây sẽ điểm qua các dạng tấn công có thể xảy ra.

a, Tấn công trực tiếp

Được sử dụng để chiếm được quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò cặp tên người sử dụng – mật khẩu. Đây là phương pháp đơn giản, dễ thực hiện và không đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Kẻ tấn

công có thể sử dụng những thông tin như tên người sử dụng, ngày sinh, địa chỉ, số nhà vv… để đoán mật khẩu. Trong trường hợp có được danh sách người sử dụng và những thông tin về môi trường làm việc, có một chương trình tự động hóa về việc dò tìm mật khẩu này, kẻ truy cập bất hợp pháp sẽ truy cập vào tài nguyên của người sử dụng để ăn cắp thông tin và phá hoại dữ liệu.

b, Tấn công nghe trộm

Việc tấn công nghe trộm trên mạng có thể mang lại những thông tin có ích như tên – mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng.

Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa vỉ giao tiếp mạng (NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng. Những thông tin này cũng có thể dễ dàng lấy được trên mạng Internet.

c, Giả mạo địa chỉ

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

d, Vô hiệu hóa các chức năng của hệ thống

Đây là kiểu tấn công nhằm làm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó được thiết kế hoạt động. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng. Ví dụ sử dụng đồng thời lệnh *ping* với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

e, Lỗi của người quản trị

Đây không phải là một kiểu tấn công của những kẻ đột nhập, tuy nhiên lỗi của người quản trị hệ thống thường tạo ra những lỗ hổng cho phép kẻ tấn công sử dụng để truy nhập vào mạng nội bộ.

2.2.3. Chức năng chính của tường lửa

Tường lửa là một thành phần đặt giữa Intranet và Internet để kiểm soát tất cả các việc lưu thông và truy cập giữa chúng với nhau. Tường lửa có thể kiểm soát tất cả các khía cạnh của truyền thông qua nó và kiểm tra nguồn gốc cũng như địa chỉ đích của mỗi gói tin. Để ngăn chặn lưu lượng truy cập không được yêu cầu từ phía được yêu cầu, tường lửa giữ một bảng các thông tin có nguồn gốc từ máy đang chạy tường lửa kết nối Internet.

Nếu người sử dụng tường lửa kết nối Internet kết hợp với chia sẻ kết nối Internet, tường lửa theo dõi tất cả lưu lượng truy cập bắt nguồn từ máy tính đang chạy tường lửa kết nối Internet và chia sẻ kết nối Internet, và theo dõi tất cả lưu lượng truy cập bắt nguồn từ mạng máy tính cá nhân.

Tường lửa kết nối Internet so sánh tất cả lưu lượng đến từ Internet với các mục trong bảng. Truy cập Internet được phép chỉ khi có một mục nhập phù hợp trong bảng cho thấy rằng việc trao đổi thông tin liên lạc đã bắt đầu trong máy tính hoặc mạng riêng của người sử dụng.

Gói tin có nguồn gốc từ một nguồn bên ngoài máy tính đang chạy tường lửa kết nối Internet, chẳng hạn như từ Internet, được chuyển xuống tường lửa trừ khi người dùng tạo một mục nhập trên tab dịch vụ để cho phép chúng. Thay vì gửi cho người sử dụng thông báo về hoạt động, tường lửa âm thầm loại bỏ những tác vụ không mong muốn. Điều này đã loại bỏ những nỗ lực xâm nhập phổ biến như quét cổng. Thông báo như vậy có thể được gửi thường xuyên dễ làm phân tâm người dùng. Thay vào đó, tường lửa có thể tạo một nhật ký bảo mật do đó người dùng có thể xem các hoạt động được theo dõi bởi các bức tường lửa.

2.2.4. Phân loại tường lửa

Tường lửa có thể bao gồm phần cứng hoặc phần mềm nhưng thường là cả hai loại.

2.2.4.1. Tường lửa cứng

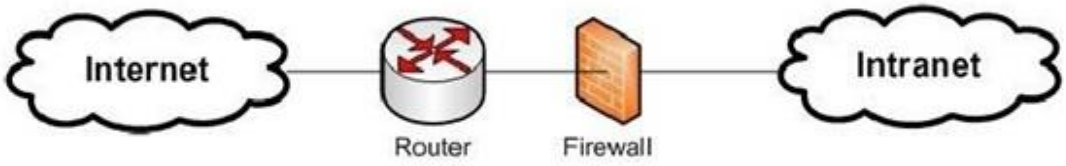
Tường lửa cứng được tích hợp trên bộ định tuyến (Router)

Đặc điểm của tường lửa cứng:

Không được linh hoạt như tường lửa mềm, không thể thêm chức năng cũng như quy tắc như tường lửa mềm.

Tường lửa cứng hoạt động ở tầng thấp hơn tường lửa mềm (Tầng Network và tầng Transport)

Tường lửa cứng không thể kiểm tra nội dung của gói tin.



Hình 2.9 - Tường lửa cứng

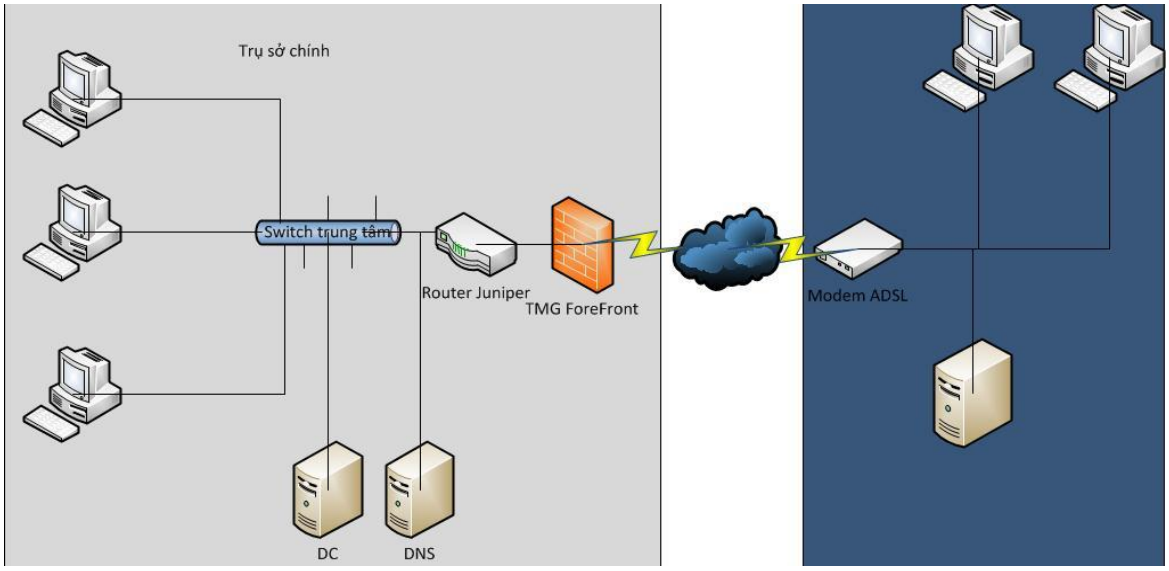
2.2.4.2. Tường lửa mềm

Đặc điểm của tường lửa mềm:

- Tính linh hoạt cao: có thể thêm, bớt quy tắc, các chức năng
- Tường lửa mềm hoạt động ở tầng cao hơn tường lửa cứng (tầng ứng dụng)
- Tường lửa mềm có thể kiểm tra được nội dung của gói tin thông qua các từ khóa.

Hình 2.10 - Tường lửa mềm

2.2.5. Mô hình tường lửa



Hình 2.11 - Mô hình tường lửa TMG

Mỗi tổ chức, mỗi công ty đều cần có một mô hình sử dụng tường lửa cụ thể để có thể đối phó với các mối nguy hiểm tiềm ẩn trên mạng Internet. Với mô hình như trên ta có thể áp dụng vào bất kỳ công ty hay tổ chức doanh nghiệp nào. Cụ thể với hệ thống bao gồm 1 máy chủ DC, quản lý tài khoản người dùng, máy chủ DNS quản lý phân giải tên miền. Switch dùng để chia mạng tới các máy client, Bộ định tuyến sử dụng để định tuyến và tường lửa được bố trí bên ngoài tất cả các thiết bị này trước khi được kết nối tới Internet. Như vậy, khi thông tin bên trong hay bên ngoài muốn trao đổi qua lại, cần phải được sự giám sát và cho phép của tường lửa mới có thể thành công được.

2.3. DÙNG CÔNG NGHỆ MẠNG RIÊNG ẢO.

2.3.1. Khái niệm mạng riêng ảo

Mạng riêng ảo (VPN) không phải là giao thức, không phải là phần mềm máy tính. VPN là một chuẩn công nghệ, cung cấp sự liên lạc an toàn giữa hai thực thể được thực hiện bằng cách mã hóa liên lạc trên một mạng không an toàn (ví dụ Internet).

Giải pháp Mạng riêng ảo được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì địa bàn hoạt động rộng (trên toàn quốc hay toàn cầu).

Trong mạng VPN:

Về cơ bản, VPN giả lập một mạng riêng trên một mạng công cộng (ví như mạng Internet). Sở dĩ nó được gọi là "ảo" bởi vì nó dựa trên các liên kết ảo (không có sự hiện diện vật lý của các liên kết này) khác với các liên kết được thiết lập trên đường thuê bao riêng. Các liên kết ảo thực chất là các dòng dữ liệu lưu chuyển trên mạng công cộng.

- Dữ liệu được đóng gói, header được cung cấp các thông tin định tuyến.

- Để đảm bảo đây là kết nối "riêng", dữ liệu được mã hóa. Các gói tin bị chặn trên mạng không thể giải mã được nếu không có khóa giải mã.

- Khi một bản tin (message) được gửi qua mạng công khai, nó được chuyển qua một số máy tính, Router, Switch hay một số thiết bị tương tự, trước khi đến được đích. Trong quá trình vận chuyển, thông điệp có thể bị chặn lại, bị sửa đổi hoặc bị đánh cắp.

Thiết lập VPN hay thực chất cung cấp sự liên lạc an toàn giữa hai thực thể được thực hiện bằng cách mã hóa liên lạc trên một mạng không an toàn, sẽ bảo đảm những yêu cầu an ninh mạng sau:

+ Tính bí mật, riêng tư (Privacy): Người không được phép không thể hiểu được sự liên lạc.

+ Toàn vẹn (Intergrity): Người không được phép không thể sửa đổi sự liên lạc.

+ Xác thực (Authenticity): Bảo đảm không xảy ra liên lạc sai địa chỉ.

- Mã hóa là việc chuyển dữ liệu có thể đọc được (clear text), về một định dạng khó thể đọc được (Ciphertext). Mã hóa theo thuật toán mã hóa và khóa bí mật. Trong các sản phẩm công nghiệp về VPN, thường hỗ trợ mã đối xứng và không đối xứng.

- Đường hầm: là kết nối giữa hai điểm cuối khi cần thiết. Kết nối này là kết nối "ảo", không phụ thuộc vào cấu trúc vật lý của mạng. Đường hầm VPN là đường hầm động , nghĩa là khi có nhu cầu trao đổi thông tin thì mới kết nối.

- Định đường hầm: là phương pháp sử dụng hạ tầng liên mạng để truyền dữ liệu của mạng này trên mạng khác. Dữ liệu chuyển tải qua mạng được đóng gói với một giao thức khác. Thay vì truyền đi gói tin được tạo ra ban đầu, giao thức tạo đường hầm đóng gói (encapsulate) gói tin với một header bổ sung. Header này cung cấp thông tin định tuyến để gói tin có thể truyền đi trên mạng. Đóng gói thực chất là mã

hóa gói dữ liệu gốc và thêm tiêu đề chứa thông tin định tuyến cho gói tin để có thể truyền qua mạng Internet. Đường hầm cũng là một đặc tính ảo trong VPN.

Các công nghệ đường hầm được dùng phổ biến hiện nay cho truy cập VPN gồm có: PPTP, L2F, L2TP hoặc IP Sec, GRE (Generic Route Encapsulation).

- Gói tin được tạo được định tuyến và truyền giữa các điểm qua mạng chung. Đường đi logic giữa điểm đầu và điểm cuối được gọi là đường hầm (Tunnel).

Để thiết lập kết nối "đường hầm", máy chủ và máy khách phải sử dụng chung giao thức đường hầm (tunnel protocol). Khi gói tin tới đích, nó được giải mã trả về nội dung ban đầu.

- Chất lượng dịch vụ (QoS - Quality of Service): Thỏa thuận về Chất lượng dịch vụ thường định ra một giới hạn cho phép về độ trễ trung bình của gói tin trong mạng. Ngoài ra, thỏa thuận này được phát triển thông qua các dịch vụ cụ thể với nhà cung cấp.

Tóm lại, **VPN** có thể nói gắn gọn là sự kết hợp:

Mã hóa + Định đường hầm + Các thỏa thuận về QoS.

2.3.2. Các loại mạng riêng ảo

Theo mục tiêu ứng dụng, VPN được phân thành hai loại:

- **VPN Site – To – Remote**:

Hỗ trợ cho người dùng từ xa hay đối tác có thể truy cập vào mạng công ty qua đường kết nối với ISP địa phương để vào Internet.

- **VPN Site – To – Site**:

Kết nối từ văn phòng chi nhánh đến văn phòng của công ty thông qua đường nối Lease Line hay DSL.

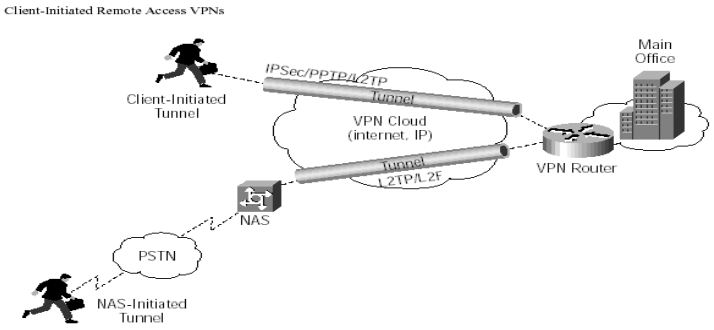
2.3.2.1. Mạng riêng ảo truy cập từ xa (Remote Access VPN)

VPN truy cập từ xa còn được gọi là mạng Dial-up riêng ảo, là một kết nối người dùng đến LAN, thường là nhu cầu của một tổ chức có nhiều nhân viên cần liên hệ với mạng riêng của mình từ rất nhiều địa điểm ở xa.

Ví dụ như công ty muốn thiết lập một VPN lớn phải cần đến một nhà cung cấp dịch vụ doanh nghiệp (ESP). ESP này tạo ra một máy chủ truy cập mạng (NAS) và cung cấp cho những người sử dụng từ xa một phần mềm máy khách cho máy tính của

họ. Sau đó, người sử dụng có thể gọi một số miễn phí để liên hệ với NAS và dùng phần mềm VPN máy khách để truy cập vào mạng riêng của công ty. Loại VPN này cho phép các kết nối an toàn, có mật mã.

Đây là kiểu mạng riêng ảo cho phép người dùng có thể thiết lập một kết nối tới máy chủ của tổ chức bằng cách sử dụng cơ sở hạ tầng được cung cấp bởi ISP. Nó cho phép người dùng có thể kết nối tới Intranet hoặc Extranet của công ty bất cứ khi nào và bất cứ ở đâu. Người dùng được phép truy cập vào tài nguyên của tổ chức như là họ kết nối trực tiếp (về mặt vật lý) vào mạng của công ty. Đường truyền trong VPN loại này có thể là tương tự, quay số hay DSL, IP di động và cáp để nối người dùng di động, máy tính từ xa hay các văn phòng lại với nhau.



Hình 2-12 : Mạng riêng ảo truy cập từ xa

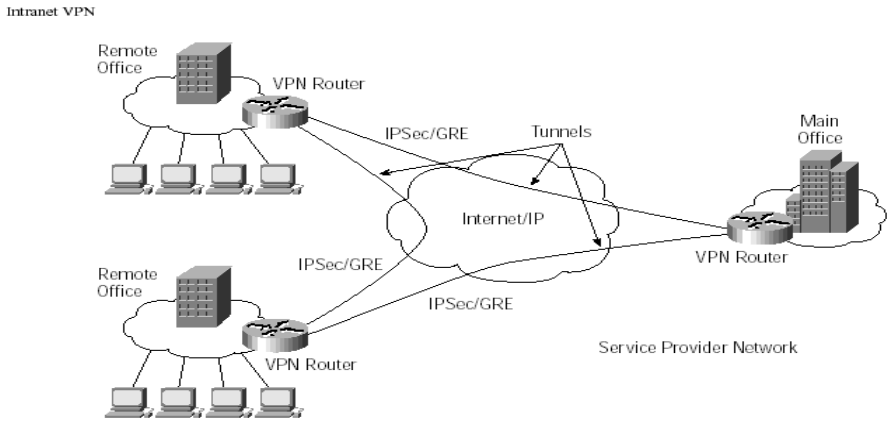
Kết nối giữa Văn phòng chính và "Văn phòng" tại gia hoặc nhân viên di động là loại VPN truy cập từ xa.

2.3.2.2. VPN điểm-nối-điểm (Site-to-Site)

VPN điểm-nối-điểm là việc sử dụng mật mã dành cho nhiều người để kết nối nhiều điểm cố định với nhau thông qua một mạng công cộng như Internet. Loại này có thể dựa trên Intranet hoặc Extranet.

Mạng riêng ảo Intranet (Intranet VPN)

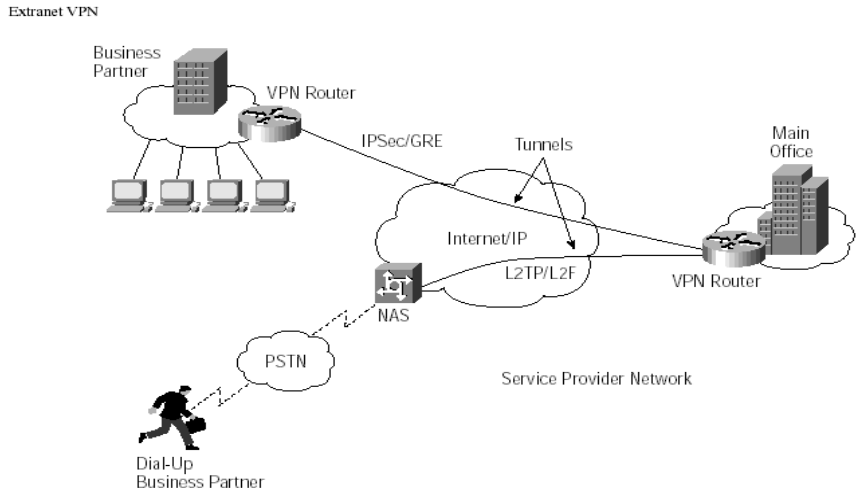
Áp dụng trong trường hợp công ty có một hoặc nhiều địa điểm ở xa, mỗi địa điểm đều đã có một mạng LAN. Khi đó họ có thể xây dựng một VPN intranet (VPN nội bộ) để kết nối các LAN đó vào trong một mạng riêng thống nhất.



Hình 2-13: Mạng riêng ảo Intranet

Mạng riêng ảo Extranet (Extranet VPN)

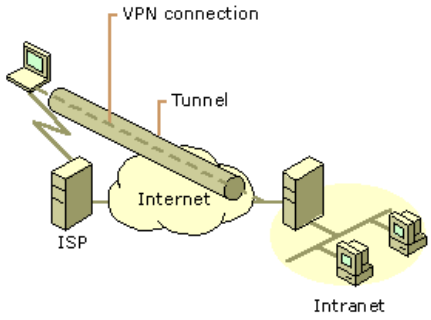
Khi một công ty có một mối quan hệ mật thiết với một công ty khác (ví dụ: một đồng nghiệp, nhà hỗ trợ hay khách hàng), họ có thể xây dựng một mạng riêng ảo Extranet để kết nối LAN của công ty mình với LAN công ty khác và cho phép các công ty đó có thể làm việc trong một môi trường có chia sẻ tài nguyên.



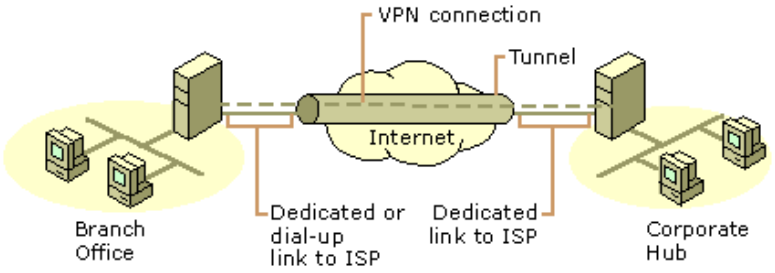
Hình 2-14: Mạng riêng ảo Extranet

Kết nối giữa Văn phòng chính và Văn phòng từ xa là loại VPN Intranet, kết nối giữa Văn phòng chính với Đối tác kinh doanh là VPN Extranet.

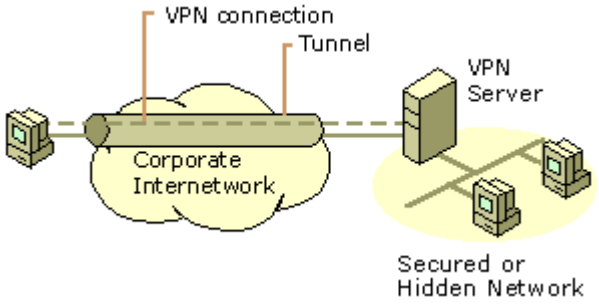
Các loại mạng riêng ảo (VPN) được mô tả trong các hình vẽ dưới đây:



Hình 2-15: Sử dụng kết nối VPN để kết nối từ xa đến Intranet



Hình 2-16: Sử dụng kết nối VPN để kết nối 2 site ở xa



Hình 2-17: Sử dụng kết nối VPN để kết nối tới mạng được bảo mật

2.3.3. Các thành phần cần thiết tạo nên một VPN

VPN bao gồm 4 thành phần chính: Internet, Security Gateway, Security Policy Server và Certificate Authority.

- Internet: Bao gồm các nhà cung cấp dịch vụ Internet với các thiết bị lớn, cao cấp, hiện đại. Các ISP có thể được phân cấp thành nhiều lớp: bậc 1, bậc2,…

- Security Gateway: Được đặt giữa các mạng công cộng và mạng riêng, ngăn chặn xâm phạm trái phép vào mạng riêng. Chúng cung cấp khả năng tạo đường hầm và mã hóa dữ liệu trước khi chuyển đến mạng công cộng. Thường là các bộ định tuyến, tường lửa, phần mềm tích hợp VPN và phần mềm VPN.

- Security Policy Server: Máy chủ bảo quản các danh sách điều khiển truy cập và thông tin khác liên quan đến người dùng mà cổng nối dùng để xác định lưu lượng nào được phép, chẳng hạn, nếu dùng PPTP, việc truy cập có thể điều khiển qua một máy chủ RADIUS.

- Certificate Authority: Máy server hoặc đơn vị thứ 3 để cấp và kiểm soát CA.

Hiện nay có nhiều loại công nghệ, giải pháp VPN, tuy nhiên các giải pháp VPN đều phải đáp ứng các yêu cầu:

- Xác thực người dùng (User Authentication)

Cung cấp cơ chế chứng thực người dùng, nghĩa là chỉ cho phép người dùng hợp lệ kết nối và truy cập hệ thống VPN.

- Điều khiển truy cập (Access Controlling)

Cung cấp địa chỉ IP hợp lệ cho người dùng sau khi gia nhập hệ thống VPN để có thể truy cập tài nguyên trên VPN.

- Mã hóa dữ liệu (Data Encryption)

Cung cấp giải pháp mã hóa dữ liệu trong quá trình truyền nhằm đảm bảo tính bảo mật và toàn vẹn dữ liệu.

- Quản lý khóa (Key Management)

Cung cấp giải pháp quản lý các khóa dùng trong quá trình mã hóa và giải mã dữ liệu.

2.3.3.1. Xác thực người dùng

Cơ chế xác thực người dùng thường được triển khai tại các điểm truy cập và được dùng để xác thực cho người dùng truy cập vào tài nguyên bên trong mạng. Chỉ có người dùng hợp lệ thì mới có thể truy cập vào bên trong mạng, điều này làm giảm đáng kể sự truy cập bất hợp pháp vào những dữ liệu được lưu trữ trên mạng.

Một số cách xác thực thường được sử dụng riêng biệt hoặc có thể được kết hợp với một số cách khác bao gồm những cách sau đây:

- Login ID and password : Phương pháp này sử dụng cơ chế xác nhận ID và mật khẩu cơ bản của hệ thống để xác nhận quyền truy cập của người dùng tại các điểm VPN.

- S/Key password : Phương pháp này khởi tạo một S/KEY bằng cách lựa chọn một mật mã bí mật và một con số tự nhiên. Số tự nhiên này bao hàm cả số lần của một hàm băm mật (MD4) sẽ được sử dụng vào mật khẩu bí mật. Khi người dùng login vào hệ thống, máy chủ sẽ cấp phát một hiệu lệnh kiểm soát. Chương trình máy khách sẽ yêu cầu nhập mật khẩu bí mật, gây ra n-1 lần lặp lại hàm băm đến nó và gửi trả lại máy chủ. Máy chủ sẽ ứng dụng hàm băm này vào thông tin được gửi lại, nếu cả hai giá trị đều giống nhau, người dùng sẽ được xác nhận thành công. Máy chủ sẽ lưu lại thông tin mà người dùng gửi cho và giảm bộ đếm mật khẩu.

- RADIUS: RADIUS là một giao thức bảo mật trên Internet khá mạnh dựa trên mô hình Client/Server, phía client sẽ truy xuất vào mạng và RADIUS server là khúc mạng cuối sẽ xác nhận client. Thông thường, RADIUS server xác nhận người dùng bằng Username và Password mà nó lưu trữ trong danh sách sẵn có.

- Two-Factor Token-Based Technique: Giống như tên gọi ám chỉ, kế hoạch này triển khai phương pháp xác nhận đôi để xác nhận những tài liệu đáng tin của người dùng. Nó kết hợp tiện ích một của token và một của password. Trong suốt quá trình xử lý, các thiết bị điện tử phần cứng cơ bản phục vụ như token và ID duy nhất, ví dụ như Personal Identification Number (PIN) được sử dụng như mật khẩu. Theo truyền thống, token sẽ là thiết bị phần cứng (có thể là một thẻ card), nhưng một số nhà cung cấp lại yêu cầu sử dụng phần mềm để làm token.

2.3.3.2. Điều khiển quyền truy nhập (Access Controlling)

Sau khi người dùng đã được xác nhận, mặc định người đó được phép truy cập vào những tài nguyên, dịch vụ và những ứng dụng được đặt trên mạng.

Điều này chứng tỏ rằng có một mối đe dọa lớn từ phía người dùng, cho dù đã được uỷ nhiệm, có thể cố ý hoặc không cố ý làm xáo trộn dữ liệu trên mạng. Bằng cách sàng lọc tài nguyên có thể hạn chế được việc này.

Controlling Access Rights cũng là một phần tích hợp của controlling access. Mối đe dọa bảo mật có thể được giảm xuống nếu ta giới hạn một số quyền truy cập đối với người dùng.

Ngày nay, một số kỹ thuật cải tiến đã cho phép độ an toàn cao hơn do việc kết hợp nhiều yếu tố như địa chỉ IP nguồn và đích, địa chỉ cổng, và group, ngày, giờ, thời gian và các ứng dụng v.v…

2.3.3.3. Mã hóa dữ liệu (Data Encryption)

Mã hóa là một trong những thành phần cơ bản của bảo mật VPN.

- Các giao thức tạo đường hầm hỗ trợ phương thức mã hóa dữ liệu cơ bản dựa trên PPP như Microsoft Point to Point Encryption – MPPE dựa trên thuật toán RSA/RC4 sử dụng khóa mã có độ dài 40-bit, 56-bit hoặc 120-bit.

- IPSec cung cấp khả năng mã hóa dữ liệu bằng IPSec Securrity. Thông thường IPSec sử dụng Encryption Standard (DES) – là mật mã kiểu khối sử dụng khóa 56-bit đối với DES hoặc 3 x 56-bit đối với 3-DES. Các mật mã khối mã hóa dữ liệu thành các khối rời rạc (các khối 64-bit trong trường hợp sử dụng DES).

- Do Internet là môi trường có thể tạo kết nối VPN từ bất cứ nơi đâu, mạng cần có các tính năng an toàn đủ mạnh để tránh các truy cập trái phép tới mạng riêng và bảo vệ dữ liệu trong quá trình truyền tải trên mạng công cộng. Ngoài các vấn đề về xác thực và mã hóa cơ bản như nêu trên, cần bổ sung một số khả năng xác thực và mã hóa mạnh hơn. Một số công nghệ xác thực và mã hóa có thể kể đến bao gồm:
Symmetric vs. Asymmetric Encryption (Private Key vs. Public Key)

+ Certificates
+ Extensible Authentication Protocol (EAP)
+ . . .

Trong VPN, hai thuật toán mã hóa bất đối xứng được dùng phổ biến là Diffie-Hellman (DH) và Rivest Shamir Adlman (RSA)

2.3.3.4. Quản lý khóa (Key Management)

Public Key Infrasture - PKI là một khuôn khổ của những chính sách để quản lý những khóa và thiết lập một phương pháp an toàn cho sự trao đổi dữ liệu. Để cải tiến việc quản lý các khóa và tính bảo mật cao trong các cuộc trao đổi dữ liệu. Một PKI được dựa trên khuôn khổ bao gồm những chính sách và thủ tục được hỗ trợ bởi các tài nguyên phần cứng và phần mềm. Những chức năng chính của PKI là:

+ Phát sinh một cặp khóa riêng và khóa chung cho PKI client
+ Tạo và xác nhận chữ ký điện tử
+ Đăng ký và xác nhận những người dùng mới
+ Cấp phát chứng nhận cho người dùng
+ Đánh dấu những khóa đã cấp phát và bảo trì quá trình sử dụng của mỗi khóa (được dùng để tham khảo về sau)
+ Hủy bỏ những đăng ký sai và hết hạn
+ Xác nhận PKI client

2.4. DÙNG CÔNG NGHỆ MÃ HÓA.

2.4.1. Mã hóa

2.4.1.1. Tổng quan về mã hóa

Để đảm bảo An toàn thông tin lưu trữ trong máy tính (giữ gìn thông tin cố định) hay đảm bảo An toàn thông tin trên đường truyền tin (trên mạng máy tính), người ta phải "che giấu" các thông tin này.

"Che" thông tin (dữ liệu) hay "mã hóa" thông tin là thay đổi hình dạng thông tin gốc, và người khác "khó" nhận ra.

"Giấu" thông tin (dữ liệu) là cất giấu thông tin trong bản tin khác, và người khác cũng "khó" nhận ra.

Vậy mã hóa là phương pháp biến đổi thông tin (phim, ảnh, văn bản, …) từ dạng bình thường sang dạng thông tin "khó" có thể hiểu được, nếu không có phương tiện giải mã. Giải mã là chuyển thông tin đã được mã hóa về dạng thông tin ban đầu (thông tin gốc), đây là quá trình ngược của mã hóa.

a. Hệ mã hóa

Việc mã hóa phải theo quy tắc nhất định, quy tắc đó gọi là Hệ mã hóa. Hệ mã hóa được định nghĩa là bộ năm thành phần P, C, K, E, D, trong đó:

P là tập hữu hạn các ký tự bản rõ

C là tập hữu hạn các ký tự bản mã

K là tập hữu hạn các khóa

E là tập các ánh xạ từ P vào C được gọi là hàm lập mã

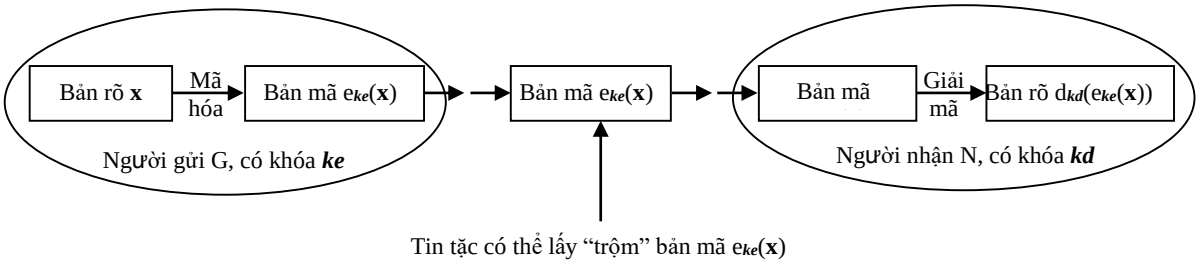
D là tập các ánh xạ từ C vào P được gọi là hàm giải mã.

Với mỗi khóa lập mã ke $\in$ K, có hàm lập mã $e_{ke} \in E$, $e_{ke}: P \rightarrow C$

Với mỗi khóa giải mã kd $\in$ K, có hàm giải mã $d_{kd} \in D$, $d_{kd}: C \rightarrow P$ sao cho $d_{kd}(e_{ke}(x)) = x, \forall x \in P$

Ở đây x được gọi là bản rõ, $e_{ke}(x)$ được gọi là bản mã.

b. Mã hóa và giải mã



Người gửi G muốn gửi bản tin **x** cho người nhận N. Để đảm bảo bí mật, G mã hóa bản tin **x** bằng khóa lập mã ***ke***, thu được bản mã $e_{ke}(\mathbf{x})$ và gửi cho N bản này.

Trên đường truyền, bản tin $e_{ke}(\mathbf{x})$ có thể bị trộm, nhưng cũng "khó" hiểu được bản tin gốc **x** nếu không có khóa giải mã ***kd***.

Khi nhận được bản mã $e_{ke}(\mathbf{x})$ mà G gửi cho, N tiến hành giải mã bằng khóa ***kd***, thu được bản tin gốc $d_{kd}(e_{ke}(\mathbf{x})) = \mathbf{x}$

2.4.2. Hệ mã hoá khoá công khai RSA

RSA là hệ mã hoá khóa công khai, độ an toàn của hệ dựa vào bài toán khó: "Phân tích số nguyên thành tích các thừa số nguyên tố".

Sơ đồ:

+ Sinh khóa:

- Chọn ngẫu nhiên, bí mật, độc lập hai số nguyên tố lớn p và q với $p \neq q$
- Tính: n = p.q. Công khai n. Đặt P = C = Z_n
- Tính bí mật giá trị: $\phi(n) = (p-1).(q-1)$
- Chọn số tự nhiên e thỏa mãn $e < \phi(n)$, e nguyên tố cùng nhau với $\phi(n)$.
- Tìm d là phần tử nghịch đảo của e theo mod $\phi(n)$: $e.d \equiv 1 (\text{mod } \phi(n))$

Khi đó, e là khoá lập mã được công khai; d là khoá giải mã phải giữ bí mật.

+ Lập mã:

Chọn P = C = Z_n với $n = p.q,\ Z_n = \{0,1,2,...,n-1\}$

$x \in P$, $y = e_k(x) = x^e \bmod n$

+ Giải mã:

$y \in C$, $x = d_k(y) = y^d \bmod n$

Ví dụ:

+ Sinh khóa:

- Chọn p = 13, q = 19
- Tính: n = p.q = 13.19 = 247. Công khai n. Đặt P = C = Z_n ={0,1,2,…, 246}
- Tính bí mật $\phi(n) = (p-1).(q-1) = 12.18 = 216$
- Chọn số tự nhiên e = 17 thỏa mãn $e < \phi(n)$, $(e, \phi(n)) = 1$
- Tìm d là phần tử nghịch đảo của e theo mod $\phi(n)$: $e.d \equiv 1 (\text{mod } \phi(n))$ ta được d = 89.

Khi đó, e = 17 là khoá lập mã được công khai; d = 89 là khoá giải mã, phải giữ bí mật.

+ Lập mã:

Chọn P = C = Z_n ={0,1,2,…, 246}

$x = 25 \in P$, mã hóa x : $y = e_k(x) = x^e \bmod n = 25^{17} \bmod 247 = 168$

+ Giải mã:

$y = 168 \in C$, giải mã y : $d_k(y) = y^d \bmod n = 168^{89} \bmod 247 = 25 = x$

Độ an toàn

1. Hệ mã hóa RSA là tất định, tức là bản rõ x và một khóa bí mật a, thì chỉ có một bản mã y.

2. Hệ mật RSA an toàn, khi giữ được bí mật khóa giải mã a, p, q, $\phi(n)$.

Nếu biết được p, q thì thám mã dễ dàng tính được $\phi(n) = (q-1)*(p-1)$.

Nếu biết được $\phi(n)$, thì thám mã tính được a theo thuật toán Euclide mở rộng. Nhưng phân tích n thành tích của p và q là bài toán "khó".

Độ an toàn của Hệ mật RSA dựa vào khả năng giải bài toán phân tích số nguyên dương n thành tích của 2 số nguyên tố lớn p và q.

2.4.3. Chữ ký số

2.4.3.1. Khái niệm chữ ký số:

a. Giới thiệu:

Để chứng thực nguồn gốc hay hiệu lực của một tài liệu, lâu nay người ta dùng chữ ký "tay", ký vào phía dưới của mỗi tài liệu. Vì vậy người ký phải ký tay trực tiếp vào tài liệu.

Ngày nay, các tài liệu được số hóa người ta cũng có nhu cầu chứng thực nguồn gốc hay hiệu lực của các tài liệu này. Rõ ràng không thể "ký tay" vào tài liệu vì chúng không được in ra trên giấy. Tài liệu "số" hay tài liệu "điện tử" là một xâu các bit (0 hay 1), xâu bit có thể rất dài nếu in trên giấy có thể lên đến hàng nghìn trang. "Chữ ký" để chứng thực một xâu bit tài liệu cũng không thể là một xâu bit nhỏ đặt phía dưới xâu bit tài liệu. Một "chữ ký" như vậy chắc chắn sẽ bị kẻ gian sao chép để làm giả chữ ký cho một tài liệu "số" bất hợp pháp.

"Chữ ký số" để chứng thực một tài liệu "số" đó chính là bản mã của xâu bit tài liệu. Người tạo ra "chữ ký số" (chữ ký điện tử) trên tài liệu "số" giống như tạo ra "bản mã" của tài liệu với khóa lập mã.

Như vậy, ký "số" trên tài liệu "số" là ký trên từng bit tài liệu. Kẻ gian khó giả mạo "chữ ký số" nếu không biết khóa lập mã.

Để kiểm tra một "chữ ký số" thuộc về tài liệu "số", người ta giải mã "chữ ký số" bằng khóa giải mã, sau đó so sánh với tài liệu gốc.

Ngoài ý nghĩa để chứng thực nguồn gốc hay hiệu lực của các tài liệu "số" mặt mạnh của "chữ ký số" hơn "chữ ký tay" là ở chỗ người ta có thể ký vào các tài liệu từ rất xa trên các mạng công khai. Hơn thế nữa, có thể ký bằng các thiết bị cầm tay (như điện thoại di động), tại khắp mọi nơi và di động, miễn là kết nối được vào mạng, giảm thiểu rất nhiều về thời gian, công sức, chi phí … so với ký tay.

"Chữ ký số" thực hiện ký trên từng bit tài liệu nên độ dài của chữ ký số ít nhất cũng bằng độ dài của tài liệu. Do đó thay vì ký trên tài liệu dài, người ta thường dùng hàm băm để tạo đại diện cho tài liệu, sau đó mới ký lên đại điện tài liệu này.

b. Sơ đồ chữ ký số:

Sơ đồ chữ ký số là bộ năm (**P, A, K, S, V)** trong đó:

P: tập hữu hạn các thông điệp.

A: tập hữu hạn các chữ kí.

K: tập hữu hạn các khoá (không gian khoá).

S : tập các thuật toán ký.

V: tập các thuật toán kiểm thử.

Với mỗi khóa k ∈ **K** tồn tại thuật toán kí $sig_k \in$ **S** và một thuật toán kiểm tra chữ ký $ver_k \in$ **V.**

Mỗi $sig_k : P \to A$ và $ver_k : P \times A \to \{true, false\}$ là những hàm sao cho mỗi thông điệp x ∈ **P** và mỗi chữ ký y ∈**A** thoả mãn phương trình dưới đây:

$$ver(x, y) = \begin{cases} true & khi\ y = sig(x) \\ false & khi\ y \neq sig(x) \end{cases}$$

Chú ý:

Người ta thường dùng hệ mã hóa khóa công khai để lập sơ đồ chữ ký số. Ở đây khóa bí mật a dùng làm khóa ký, khóa công khai b dùng để kiểm tra chữ ký.

Ngược với việc mã hóa: dùng khóa công khai b để mã hóa, dùng khóa bí mật a để giải mã. Điều này hoàn toàn tự nhiên vì "ký" để xác định người ký hay hiệu lực của tài liệu nên "ký" cần bí mật. Còn sau khi ký, tài liệu hay chữ ký là công khai cho mọi người biết nên họ dùng khóa công khai b để kiểm tra chữ ký.

2.4.3.2. Sơ đồ ký số RSA

Sơ đồ chữ ký RSA được cho bởi bộ năm: S = (**P, A, K, S, V**).

- Tạo cặp khóa:

P = **A** = Z_n, với n = p.q, p và q là các số nguyên tố lớn.

$\phi(n) = (p-1)(q-1)$ K = (n, p, q, a, b)

Chọn b $\in Z_n$ nguyên tố cùng nhau với $\phi(n)$

Chọn a $\in Z_n$ là nghịch đảo của b theo module $\phi(n)$

Các giá trị n và b công khai; các giá trị p, q, a bí mật.

- ***Ký số:*** Sử dụng cặp (n, a) để ký

Với mỗi K = (n, p, q, a, b) và x $\in Z_n$ ta định nghĩa chữ ký là:

$y = sig_k(x) = x^a \bmod n$, y $\in$ A

- ***Kiểm tra chữ kí:*** Sử dụng cặp (n, b) để kiểm tra chữ ký

$Ver_k(x, y) = true \Leftrightarrow x \equiv y^b \pmod n$

Ví dụ: Tạo chữ ký trên văn bản x = 2.

- Tạo cặp khóa:

Chọn p = 3, q = 5. Tính n = p.q = 15

P = **A** = Z_n ={ 0, 1, 2, …, 14}

Tính $\phi(n) = (p-1)(q-1) = 8$

Chọn b = 3 $\in Z_n$ thỏa mãn $(b, \phi(n))=1$

Tìm a $\in Z_n$ là nghịch đảo của b theo module $\phi(n)$, ta được a = 3

Khi đó công khai (b, n), bí mật (p, q, a)

- ***Ký số:*** Sử dụng cặp (n, a) = (15, 3) để ký.

x =2 $\in$ P ta thu được chữ ký là: $y = sig_k(x) = x^a \pmod{15} = 2^3 \pmod{15} = 8$

Vậy chữ ký là: $y = sig_k(x) = 8 \in A$.

Người ký gửi cặp (x, y) đi.

- ***Kiểm tra chữ ký:*** Sử dụng cặp (n,b) để kiểm tra chữ ký

Tính $x' = y^b \bmod n = 8^3 \bmod 15 = 2$

Vậy Ver(x,y)= true (vì x' = x). Do đó chữ ký là đúng, không bị giả mạo.

2.4.4. Hàm băm

2.4.4.1. Tổng quan về hàm băm

"Hàm băm" là thuật toán không dùng khóa để ***mã hóa*** nó có nhiệm vụ "lọc" (băm) tài liệu (bản tin) và cho kết quả là một giá trị "băm" có kích thước cố định, còn gọi là "***đại diện tài liệu***" hay "đại diện bản tin", "đại diện thông điệp".

Hàm băm là hàm một chiều, theo nghĩa giá trị của hàm băm là duy nhất và từ giá trị băm này, "khó thể" suy ngược lại được nội dung hay độ dài ban đầu của tài liệu gốc.

1./ Đặc tính của hàm băm

Hàm băm **h** là hàm một chiều có các đặc tính sau:

* Với tài liệu đầu vào (bản tin gốc) x, chỉ thu được giá trị băm duy nhất **z = h(x)**

* Nếu dữ liệu của trong bản tin x bị thay đổi hay bị xóa để thành bản tin x', thì giá trị băm **h(x') ≠ h(x)**

* Nội dung của bản tin gốc "khó" thể suy ra từ giá trị hàm băm của nó. Nghĩa là với thông điệp x thì dễ tính được **z = h(x)**, nhưng lại khó tính ngược lại được x nếu chỉ biết giá trị băm **h(x)** (Kể cả khi biết hàm băm h)

2./ Ứng dụng của hàm băm

* Với bản tin dài x, thì chữ ký trên x cũng sẽ dài, như vậy sẽ tốn thời gian "ký", tốn bộ nhớ lưu trữ "chữ ký", tốn thời gian truyền "chữ ký" trên mạng. Người ta dùng hàm băm **h** để tạo đại diện cho bản tin **z = h(x)**, nó sẽ có độ dài ngắn. Sau đó ký trên z, như vậy chữ ký trên z sẽ nhỏ hơn nhiều so với chữ ký trên bản tin gốc x.

* Hàm băm dùng để xác định tính toàn vẹn dữ liệu.

* Hàm băm dùng để bảo mật một số dữ liệu đặc biệt, ví dụ như bảo vệ mật khẩu, bảo vệ mật mã.

3./ Các loại hàm băm

Các hàm băm dòng MD (MD2, MD4, MD5) do Rivest đề xuất. Giá trị năm theo các thuật toán này có độ dài cố định là 128 bit. Hàm băm MD4 đưa vào năm 1990. Một năm sau phiên bản mạnh hơn là MD5 được đề xuất.

Hàm băm an toàn SHA, phức tạp hơn nhiều, cũng dựa trên các phương pháp tương tự, được công bố trong Hồ sơ Liên bang năm 1992 và được chấp nhận làm tiêu chuẩn vào năm 1993 do Viện Tiêu Chuẩn và Công Nghệ Quốc Gia (NIST). Giá trị băm theo thuật toán này có độ dài cố định là 160 bit.

2.4.5. Kỹ thuật mã khóa EC- ELGAMAL

2.4.5.1. Hệ mã hóa Elgamal cổ điển

Sơ đồ (Elgamal đề xuất năm 1985)

a/. *Sinh khóa* (***bí mật, công khai***) ***(a, h)*** :

Chọn số nguyên tố p sao cho bài toán logarit rời rạc trong Z_p là "khó" giải. Chọn phần tử nguyên thuỷ $g \in Z_p^*$.

Đặt $P = Z_p^*$, $C = Z_p^* \times Z_p^*$.

Chọn khóa bí mật là $a \in Z_p^*$. Tính khóa công khai $h \equiv g^a \mod p$.

Định nghĩa tập khóa: $K = \{(p, g, a, h): h \equiv g^a \mod p\}$.

Các giá trị p, g, h được công khai, phải giữ bí mật a.

Với ***Bản rõ*** $x \in P$ và ***Bản mã*** $y \in C$, với khóa $k \in K$ định nghĩa:

b/. *Lập mã*:

Chọn ngẫu nhiên bí mật $r \in Z_{p-1}$, bản mã là $y = e_k(x, r) = (y_1, y_2)$

Trong đó $y_1 = g^r \pmod p$ và $y_2 = x * h^r \pmod p$

c/. *Giải mã*: $d_k(y_1, y_2) = y_2 (y_1^a)^{-1} \pmod p = x$.

Ví dụ

*** Bản rõ** $x = 1985$.

Chọn $p = 2110$, $g = 2$, $a = 365$.

Tính khóa công khai $h = 2^{365} \mod 2110 = 882$.

*** Lập mã**: Chọn ngẫu nhiên $r = 503$.

Bản mã là $y = (1188, 1870)$, trong đó

$y_1 = 2^{503} \mod 2110 = 1188$ và $y_2 = 1985 * 882^{503} \mod 2110 = 1870$

*** Giải mã**: $x = y_2 (y_1^a)^{-1} \mod p$

$= 1870 * (1188^{365})^{-1} \mod 2110 = 1985$.

Độ an toàn

a/. Hệ mã hóa Elgamal là không tất định, tức là với một bản rõ x và 1 khóa bí mật a, thì có thể có nhiều hơn một bản mã y, vì trong công thức lập mã còn có thành phần ngẫu nhiên r.

b/. Độ an toàn của Hệ mật Elgamal dựa vào khả năng giải bài toán logarit rời rạc trong Z_p. Theo giả thiết trong sơ đồ, thì bài toán này phải là "khó" giải.

Cụ thể như sau:

Theo công thức lập mã: $y = e_k(x, r) = (y_1, y_2)$, trong đó

$y_1 = g^r \bmod p$ và $y_2 = x * h^r \bmod p$

Như vậy muốn xác định bản rõ x từ công thức y_2, thám mã phải biết được r.

Giá trị này có thể tính được từ công thức y_1, nhưng lại gặp bài toán logarit rời rạc.

2.4.5.2. Hệ mã hóa EC-ElGamal

Hệ mã hóa EC-ElGamal là một sự thích ứng của hệ mã hóa ElGamal trên đường cong elliptic. Nó không những giữ được tính chất đồng cấu, mà bài toán logarit rời rạc trên nhóm các điểm trên một đường cong elliptic là khó giải hơn trong vành modun các số nguyên.

Hệ mã hóa trên đường cong Elliptic là một hệ mã hóa công khai. Trong hệ mã hóa công khai, mỗi user hoặc thiết bị tham gia giao tiếp thường có một cặp khóa, một công khai và một bí mật. Chỉ có những người dùng cụ thể biết khóa riêng trong khi khóa công khai được phân phối cho tất cả người dùng tham gia vào các giao tiếp. Một số thuật toán khóa công khai có thể yêu cầu một tập các hằng số được xác định trước để các thiết bị tham gia vào các giao tiếp có thể biết đến (ví dụ như miền thông số của đường cong là các hằng số được xác định trước).

Hệ mã hóa trên đường cong Elliptic có thể thực hiện trong 3 trường. Trường số thực, trường nguyên tố (là trường hữu hạn *Fp* với *p* là số nguyên tố), trường nhị phân. Phép toán chính trên đường cong là phép cộng, phép nhân, phép nhân đôi trên tọa độ các điểm.

Các phép toán này có thể thực hiện trên tất cả các trường. Tuy nhiên trong mã hóa, hệ thống xử lý trên trường nguyên tố được sử dụng nhiều hơn cả, nó phù hợp cho mục đích xây dựng các phần mềm. Sơ đồ dưới đây đưa ra mô hình phân cấp của hệ mã hóa trên đường cong Elliptic.

<table>
<tr><td colspan="3">Elliptic Curve Cryptography</td></tr>
<tr><td colspan="3">Fields</td></tr>
<tr><td>Real number field</td><td>Prime field</td><td>2^m galois field</td></tr>
<tr><td>Point Addition</td><td>Point Multiplication</td><td>Point doubling</td></tr>
<tr><td></td><td>Cryptographic algorithms</td><td></td></tr>
</table>

Trong trường nguyên tố, cho **p là số nguyên tố**, (p>3). Một đường cong Elliptic trên trường F_p được định nghĩa bởi dạng: $\boldsymbol{y^2 = x^3 + ax + b \ (mod\ p)}$, (1) trong đó $\boldsymbol{a, b \in F_p}$ và $4a^3 + 27b^2 \not\equiv 0\ (mod\ p)$.

(Số lượng điểm của $E(F_p)$ thỏa mãn: $p + 1 - 2\sqrt{p} \leq \#E(Fp) \leq p + 1 + 2\sqrt{p}$).

Đường cong Elliptic trên trường hữu hạn F_p

1./ Định nghĩa

Cho *p* là số nguyên tố (*p*>3). Một đường cong Elliptic trên trường F_p được xác định bởi tập T:

T = (*p*,*a*,*b*,*G*,*n*,*h*). Trong đó:

- *p* là một số nguyên tố xác định trường hữu hạn F_p,
- Hai tham số *a*,*b* là tham số của phương trình Weierstrass:

$$y^2 = x^3 + ax + b$$

trong đó $a, b \in F_p$ và $4a^3 + 27b^2 \not\equiv 0\ (mod\ p)$

- *G* là điểm sinh có tọa độ (x_G, y_G), *G* được chọn để thực hiện các phép toán mã hóa.
- *n* là bậc của *G*.
- *h* là phần phụ đại số: $h = \#E(F_p)/n$. ($\#E(F_p)$ là số điểm của đường cong).

Định nghĩa này sẽ là cơ sở chính để xây dựng hệ mật mã dựa trên đường cong Elliptic.

Tập $E(F_p)$ bao gồm tất cả các cặp điểm (x, y), $x, y \in F_p$ thỏa mãn phương trình (1) cùng với một điểm O - gọi là điểm tại vô cực không nằm trên đồ thị.

$$S = \{(x,y): y^2 = x^3 + ax + b, x, y \in F_p\} \{O\}.$$

2./ Cấp của nhóm

Cho E là đường cong elliptic xác định trên trường F_q. Tất cả số điểm trên E(F_q) kí hiệu là # E(F_q) được gọi là cấp của E trên F_q.

Phương trình Weierstrass E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ có ít nhất hai nghiệm với mỗi $x \in F_q$, và # E(F_q) $\in [1, 2q+1]$, định lý Hasse giới hạn số lượng điểm trong khoảng.

Định lý: Cho E là đường cong elliptic xác định trên trường F_q. Khi đó Số lượng điểm của E(F_p) là #E(F_p) thỏa mãn định lý Hasse:

$$q+1-2\sqrt{q} \le \#\, E(F_q) \le q+1+2\sqrt{q}$$

Đoạn $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ được gọi là đoạn Hasse.

Nếu E được định nghĩa trên F_q thì # E(F_q) $= q+1-t$ với $|t| \le \sqrt[2]{q}$, t được gọi là vết của E trên F_q. Khi $\sqrt[2]{q}$ là tương đối nhỏ so với q, chúng ta có # E(F_q) $\approx q$. Tiếp theo, xác định các giá trị có thể cho # E(F_q) như là E chạy trên tất cả các đường cong elliptic xác định trên F_q.

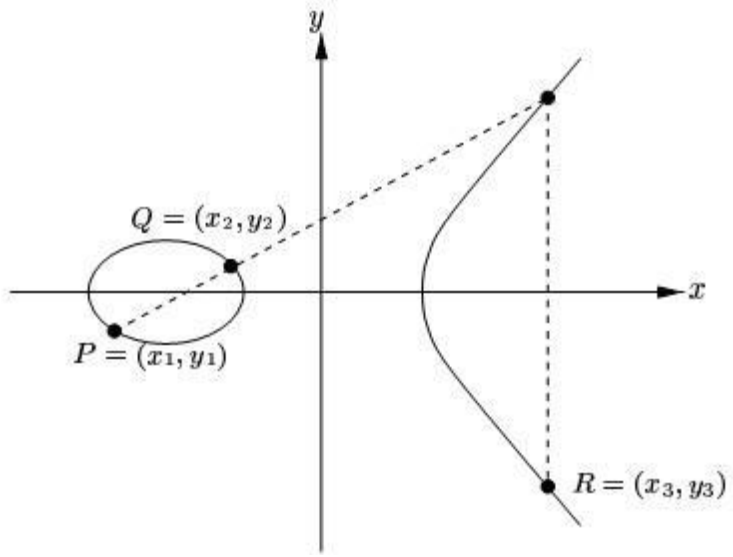
Định nghĩa: Cấp của một điểm P là số nguyên dương nhỏ nhất n sao cho $[nP] = P \oplus ... \oplus P = P_\infty$. Nếu nếu không tồn tại số n để [nP] = P_∞ thì P có cấp là ∞ . Và cấp của một phần tử trung lập P_∞ là 1.

3./ Luật nhóm

Quy tắc tiếp tuyến và dây cung: phép cộng hai điểm trên đường cong E(F_p) thành một điểm thứ ba cũng thuộc được cong Elliptic. Cùng với phép cộng này, tập hợp các điểm E(F_p) làm thành một nhóm. Nhóm này được sử dụng trong hệ mật đường cong Elliptic.

Nếu hai điểm P = (x_1, y_1) và Q = (x_2, y_2) với $x_1 \neq x_2$ nằm trên cùng một đường cong Elliptic E, thì đường thẳng qua hai điểm P và Q sẽ cắt một điểm duy nhất R = (x_3, y_3) nằm trên đường cong E.

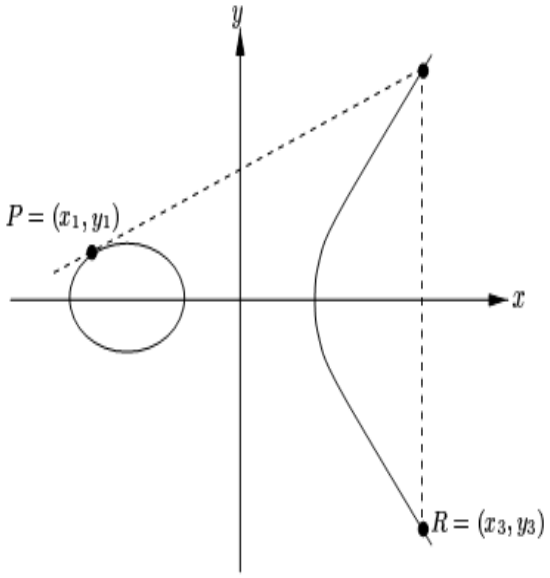
Để tìm R, ta nối P và Q bằng đường thẳng *d*. Đường thẳng này cắt E tại 3 điểm P, Q và -R(*x*,*y*). Điểm R(*x*,-*y*) sẽ có tung độ là giá trị đối của *y*.



Hình 2.18: Phép cộng trên đường cong Elliptic

Tiếp tuyến của đường cong tại điểm bất kỳ P(*x*,*y*) trên đường cong E cũng cắt đường cong tại một điểm duy nhất nằm trên E.

Ta có phép nhân đôi: Nếu cộng hai điểm P, Q∈ E với P = Q thì đường thẳng *d* sẽ là tiếp tuyến của đường cong Elliptic tại P.



Hình 2.19: Phép nhân đôi trên đường cong Elliptic

Công thức đại số cho phép cộng của hai điểm và phép nhân đôi của một điểm trên E được mô tả dưới phương diện hình học:

1. $P + O = O + P, \forall P \in E(F_p)$

2. Nếu $P = (x, y) \in E(F_p)$, thì $(x, y) + (x, -y) = O$.

Điểm $(x, -y)$ ký hiệu là -P và $-P \in E(F_p)$.

3. Cho hai điểm $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(F_p)$.

Nếu $P \neq \pm Q$ thì P+Q = (x_3, y_3) được xác định như sau:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ và } y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

4. Cho $P = (x_1, y_1) \in E(F_p), P \neq -P$. Khi đó $2P = (x_3, y_3)$ được xác định như sau:

$$x_3 = \left(\frac{3x_1^2 - a}{2y_1}\right) - 2x_1 \text{ và } y_3 = \left(\frac{3x_1^2 - a}{2y_1}\right)(x_1 - x_3) - y_1.$$

4./ Tương ứng một số với một điểm trên đường cong

Để sử dụng được ứng dụng của đường cong elliptic, chúng ta cần một phương thức để ánh xạ một thông điệp thành một điểm trên đường cong elliptic. Hệ mật đường cong elliptic sau đó sử dụng các phép toán đối với các điểm này để có được các điểm mới tương ứng như các bản mã. Giả sử m là một số nguyên dương nào đó, bản rõ m được ứng với điểm P_m trên E.

Phương thức nhúng bản rõ được Koblitz đưa ra (1997) trên đường cong E định nghĩa trên F_p, p là số nguyên tố lớn hơn 3. Cho K là số nguyên dương đủ lớn sao cho thỏa mãn xác suất sai xấp xỉ $1/2^K$. (K = 20, 30 hoặc 50 là đủ). Ý tưởng được thực hiện như sau:

Cho E: $y^2 \equiv x^3 + ax + b (\text{mod } p)$. Thông điệp m (giả sử m là một số) sẽ được nhúng trong tọa độ x của một điểm trên E. Tuy nhiên xác suất chỉ khoảng ½ rằng $m^3 + am + b$ là lấy được bình phương *mod p*. Do đó, ở đây chúng ta sẽ nối thêm vào một vài bit ở cuối m đến khi chúng ta nhận được một số x sao cho $x^3 + ax + b$ lấy được bình phương *mod p*.

Giả sử rằng m thỏa mãn $(m+1)K < p$. Thông điệp m sẽ được biểu diễn bởi số $x = mK + j$, với $0 \le j < K$. Cho $j = 0, 1, \ldots, K\text{-}1$. Tính $x^3 + ax + b$ và tìm căn bậc hai của $f(x)$. Nếu có một căn bậc hai của y thì chúng ta được $P_m = (x, y)$. Nếu kết quả $f(x)$ không là bình phương thì tăng x lên 1 và tiếp tục tính toán từ đầu cho đến khi tìm được số x sao cho $f(x)$ là một bình phương hoặc $j = K$. Nếu j không bao giờ bằng K thì sẽ không có ánh xạ một thông điệp sang một điểm. Vì $f(x)$ là một bình phương với xấp xỉ ½, nên chúng ta có khoảng $1/2^K$ khả năng để phương pháp này là sai.

Chúng ta có thể khôi phục lại được m từ điểm $P_m(x, y)$ bởi công thức:

$m = [x/K]$, trong đó $[x/K]$ biểu thị phần nguyên của x/K.

Ví dụ: Cho p = 179 và đường cong E: $y^2 = x^3 + 2x + 7$.

Chọn $K = 10$, khi đó xác suất thất bại là $1/2^{10}$.

Thông điệp m phải thỏa mãn $(m+1)K < p$, tức là $m.10 + 10 < 179$

suy ra $0 \le m \le 16$. Giả sử ta chọn thông điệp $m = 5$.

Tiếp theo, biểu diễn x dưới dạng: $x = mK + j = 5.10 + j = 50 + j$, với $j = 0, .., 9$.

Khi đó, x có thể chọn là: 50, 51, …, 59.

Cho $x = 51$. Chúng ta được $y^2 \equiv x^3 + 2x + 7 \equiv 121 \pmod{179} \equiv 11^2 \pmod{179}$.

Vậy thông điệp $m = 5$ ứng với điểm $P_m(51, 11)$ trên đường cong E.

Thông điệp m có thể được khôi phục lại bằng cách tính: $m = [x/K] = [51/10] = 5$.

5./ Định nghĩa hệ mã hóa EC-Elgamal

Hệ mã hóa EC-ElGamal được định nghĩa với tập các tham số sau:

- Xác định một trường hữu hạn, giả sử Fp với p là số nguyên tố lớn.

- Chọn một đường cong Elliptic trên Fp được xác định bởi hệ số a, b của phương trình Weierstrass.

- Xác định một nhóm con cyclic G của $E(Fp)$ và G có phần tử sinh P.

- n là bậc của P và h là phần phụ đại số của G trong $E(Fp)$: $h = \#E(Fq)/n$

Tham số của EC-ElGamal = (p, a, b, P, n, h)

Sinh khóa:

- Chọn ngẫu nhiên số nguyên d [2, n-1]

- Tính $Q = d * P$

- Khóa công khai là điểm Q và khóa bí mật là d

Mã hóa: $m \xrightarrow{encription} c$

- Chọn các tham số và khóa công khai Q

- Biểu diễn thông điệp cần mã hóa như một điểm M trên đường cong elliptic $E(Fp)$

- Chọn ngẫu nhiên số nguyên k,

- Tính $C_1 = k*P$ và $C_2 = M + k*Q$

Gửi thông điệp mã hóa: $c = (C_1, C_2) = (k*P, M + k*Q)$

Giải mã: $m \xleftarrow{decryption} c$

- Sử dụng khóa công khai x tính $d * C_1$

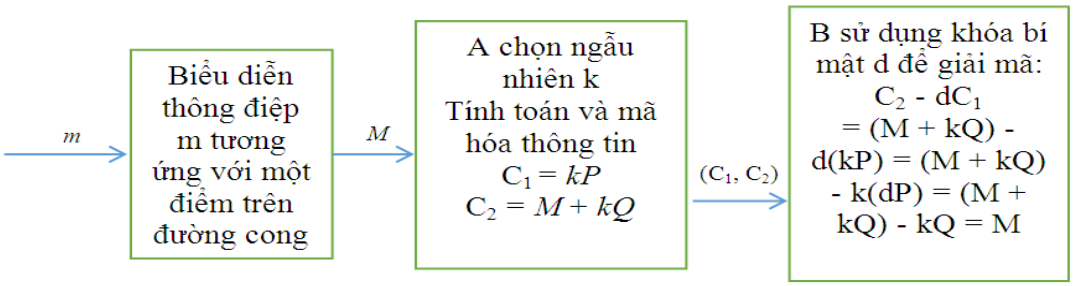
- Khôi phục M bằng cách: $M = C_2 - d * C_1$

Dễ dàng chứng minh được phép toán trả về bản rõ m:

$C_2 - d * C_1 = (M + k * Q) - d(k * P) = (M + k * Q) - k(d * P)$

$= (M + k * Q) - k * Q = M$

Ví dụ: Giả sử A và *B* muốn trao đổi thông tin mật cho nhau trên cơ sở đường cong Elliptic, thì *A* và *B* chọn đường cong Elliptic E với các hệ số *a*, *b*, modulo *p* và điểm khởi tạo $P \in E_p(a, b)$, *P* có bậc là *n* ($nP = 0$), *n* là số nguyên tố lớn. Nhóm elliptic $E_p(a, b)$ và điểm sinh *P* được công khai.



Ví dụ: Xét đường cong Elliptic: $y^2 = x^3 - x + 188$ *mod* 751.

Ta có $E_{751}(-1, 188)$, chọn điểm sinh P = (0, 376).

- Giả sử khóa bí mật của B là *d* = 85. Khi đó, khóa công khai của B là:

Q = *d*.P = 85(0,376) = (671, 558).

- A muốn gửi thông điệp *m* tới B. Giả sử thông điệp *m* được biểu diễn trên đường cong tương ứng với điểm M(443, 253) ∈ $E_{751}(-1, 188)$. Đầu tiên, A chọn ngẫu nhiên *k* = 113 và sử dụng khóa công khai của B để mã hóa M.

C_1 = *k*.P = 113(0,376) = (34, 633)

C_2 = M + *k*Q = (443, 253) + 113(671, 558) = (217, 606)

A gửi cặp (C_1, C_2) = [(34, 633) ; (217, 606)] cho B.

- B sau khi nhận được cặp bản mã (C_1, C_2), B sử dụng khóa bí mật *d* = 85 để giải mã.

B tính toán: C_2 - *d*C_1 = (M + kQ) - *d*(kP)

C_2 - *d*C_1 = (217, 606) - 85(34, 633)

C_2 - *d*C_1 = (217, 606) - (47, 416)

C_2 - *d*C_1 = (217, 606) + (47, - 416) (vì -P = (x_1, -y_1))

C_2 - *d*C_1 = (217, 606) + (47, 335)

C_2 - *d*C_1 = (443, 253) = M.

Tách *m* từ M ta sẽ được bản rõ *m*.

Chương 3: THỬ NGHIỆM ỨNG DỤNG BẢO VỆ THÔNG TIN TRÊN MẠNG MÁY TÍNH

3.1. PHÁT BIỂU BÀI TOÁN

Ngày nay trong mọi hoạt động của con người thông tin đóng một vai trò quan trọng không thể thiếu. Xã hội càng phát triển nhu cầu trao đổi thông tin giữa các thành phần trong xã hội ngày càng lớn. Mạng máy tính ra đời đã mang lại cho con người rất nhiều lợi ích trong việc trao đổi và xử lý thông tin một cách nhanh chóng và chính xác. Chính từ những thuận lợi này đã đặt ra cho chúng ta một câu hỏi, liệu thông tin đi từ nơi gửi đến nơi nhận có đảm bảo tuyệt đối an toàn, ai có thể đảm bảm thông tin của ta không bị truy cập bất hợp pháp. Thông tin được lưu giữ, truyền dẫn, cùng sử dụng trên mạng lưới thông tin công cộng có thể bị nghe trộm, chiếm đoạt, xuyên tạc hoặc phá huỷ dẫn đến sự tổn thất không thể lường được. Đặc biệt là đối với những số liệu của hệ thống ngân hàng, hệ thống thương mại, cơ quan quản lý của chính phủ hoặc thuộc lĩnh vực quân sự được lưu giữ và truyền dẫn trên mạng. Nếu như vì nhân tố an toàn mà thông tin không dám đưa lên mạng thì hiệu suất làm việc cũng như hiệu suất lợi dụng nguồn dữ liệu đều sẽ bị ảnh hưởng. Trước các yêu cầu cần thiết đó, việc mã hoá thông tin sẽ đảm bảo an toàn cho thông tin tại nơi lưu trữ cũng như khi thông tin được truyền trên mạng.

Một phương pháp đảm bảo an toàn thông tin tốt là kết hợp nhiều phương pháp an toàn bảo mật giúp cho người gửi và người nhận luôn thấy được toàn vẹn về thông tin và dữ liệu.

Xuất phát từ yêu cầu thực tế, Bob nhận được một tệp tin thông điệp từ Alice gửi đến, tuy nhiên Bob không biết được rằng tệp tin mà mình nhận được có còn nguyên vẹn không? Hay nói cách khác trong quá trình truyền tin có hay không bị các hacker tấn công thay đổi nội dung tệp tin.

Input:

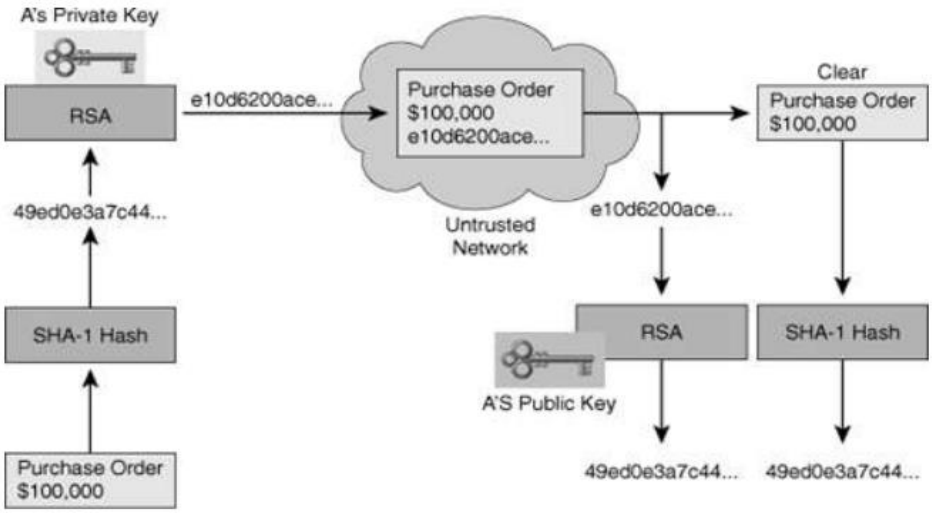
- Tệp tin của Alice gửi

Output:

- Xác minh tệp tin mà Bob nhận được từ Alice có bị thay đổi hay không?

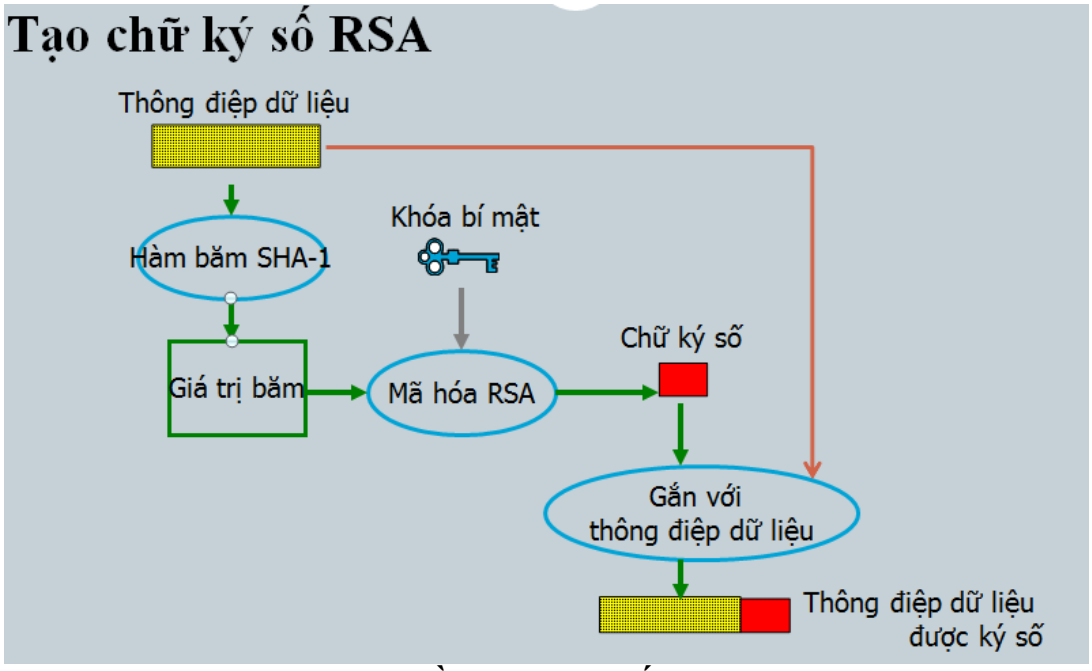
3.2. ĐỀ XUẤT GIẢI PHÁP

3.2.1. RSA + SHA-1

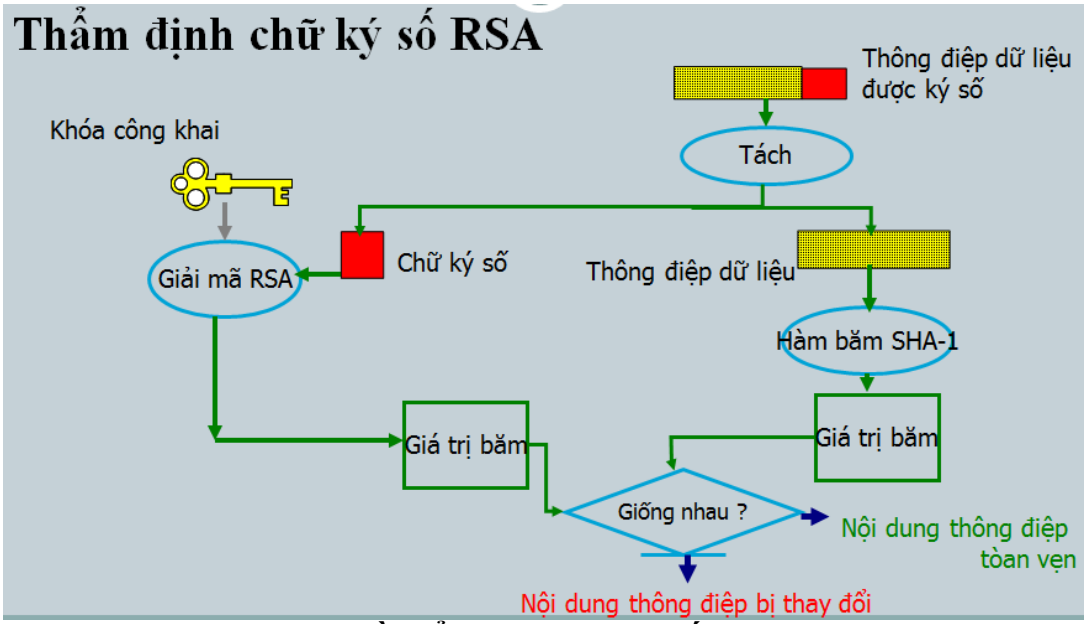


Hình 3.1. Sơ đồ thuật toán RSA + SHA-1

Cụ thể hơn:



Hình 3.2. Sơ đồ tạo chữ ký số RSA + SHA-1



Hình 3.3. Sơ đồ thẩm định chữ ký số RSA + SHA-1

a./ Quá trình ký (bên gửi)

- Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) SHA-1

- Chuỗi đại diện được ký sử dụng khóa riêng (Priavte key) của người gửi và giải thuật tạo chữ ký (Signature/ Encryption algorithm) RSA. Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa bởi giải thuật RSA (Encryted message digest)

- Thông điệp ban đầu (message) được ghép với chữ ký số(Digital signature) tạo thành thông điệp đã được ký (Signed message)

- Thông điệp đã được ký (Signed message) được gửi cho người nhận

b./ Quá trình kiểm tra chữ ký (bên nhận)

- Tách chữ ký số RSA và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;

- Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký là SHA-1)

- Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số RSA-> chuỗi đại diện thông điệp MD2

- So sánh MD1 và MD2:

+ Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).

+ Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

Ưu điểm:

Sự xuất hiện của chữ ký số và chức năng tiền định của nó, đặc biệt là vai trò của nó như là một công cụ trong việc xác định tính nguyên gốc, xác định tác giả, bảo đảm tính toàn vẹn của tài liệu số, đã đóng một vai trò vô cùng quan trọng trong việc xác định địa vị pháp lý của tài liệu số trong giao dịch số.

Việc sử dụng chữ ký số trong phần lớn trường hợp là cơ sở khẳng định giá trị pháp lý của những văn bản điện tử tương đương với tài liệu giấy. Hiện nay, chữ ký số là phương tiện duy nhất để xác nhận giá trị pháp lý của tài liệu điện tử.

Như vậy, với sự xuất hiện của chữ ký số, vấn đề giá trị pháp lý của tài liệu điện tử, có thể coi như đã được giải quyết.

Nhược điểm:

- Thông điệp dữ liệu không được mã hóa nên dễ bị tấn công nghe lén làm lộ thông tin, nhất là với các thông điệp quan trọng.

3.2.2. RSA + SHA-1 + EC-Elgamal

a. Quá trình ký và mã hóa của bên gửi

- Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) SHA-1.

- Tạo chữ ký dựa trên chuỗi đại diện vừa thu được với khóa bí mật của người gửi.

- Chuỗi đại diện và chữ ký được mã hóa theo khóa công khai của người nhận thu được chuỗi đại diện và chữ ký đã được mã hóa (Encryted message digest and Signature).

- Thông điệp được mã hóa theo khóa công khai EC-Elgamal của người nhận (Encryted EC-Elgamal Message).

- Nối chuỗi đại diện và chữ ký đã được mã hóa vào thông điệp được mã hóa và gửi tới người nhận.

b. Quá trình giải mã và xác nhập chữ ký

- Người nhận sau khi nhận được toàn bộ dữ liệu từ người gửi sẽ tiến hành tách chuỗi đại diện và chữ ký ra khỏi thông điệp được mã hóa.

- Thông điệp sẽ được giải mã với khóa bí mật EC-Elgamal để ra thông điệp ban đầu.

- Chữ ký và chuỗi đại diện được giải mã với khóa bí mật RSA, sau khi thu được bản rõ thì người nhận tiến hành so khớp chuỗi đại diện với chữ ký bằng khóa công khai của người gửi để xác minh bản chuỗi đại diện. Nếu chữ ký không khớp với chuỗi đại diện thì chứng tỏ chuỗi đại diện đã bị thay đổi, ngược lại thì thu chuỗi đại diện đúng của người gửi.

- Tiến hành tính toán chuỗi đại diện với thông điệp vừa giải mã và so sánh với chuỗi đại diện vừa thu được qua quá trình so khớp chữ ký. Nếu 2 chuỗi đại diện không khớp nhau thì kết luận thông điệp đã bị thay đổi, ngược lại kết luận thông điệp an toàn.

Ưu điểm:

- Hacker không thể nghe lén được thông điệp gửi đi vì đã được mã hóa.

Nhược điểm

- Khối lượng thông tin truyền trên đường truyền lớn.

Việc sử dụng chữ ký số trong giao dịch cũng có những ưu điểm và bất cập nhất định. Dưới đây là những hạn chế của chữ ký số:

- Sự lệ thuộc vào máy móc và chương trình phần mềm: chữ ký số là một chương trình phần mềm máy tính. Để kiểm tra tính xác thực của chữ ký cần có hệ thống máy tính và phần mềm tương thích. Đây là hạn chế chung khi sử dụng văn bản điện tử và chữ ký số.

- Tính bảo mật không tuyệt đối: Nếu chữ ký bằng tay được thực hiện trên giấy, được ký trực tiếp và luôn đi kèm với vật mang tin, chữ ký tay không thể chuyển giao cho người khác, thì chữ ký số không như vậy.

Chữ ký số là một bộ mật mã được cấp cho người sử dụng, đây là phần mềm máy tính không phụ thuộc vào vật mang tin. Chính vì vậy, trở ngại lớn nhất khi sử dụng chữ ký số là khả năng tách biệt khỏi chủ nhân của chữ ký. Nói cách khác, chủ nhân của chữ ký số không phải là người duy nhất có được mật mã của chữ ký. Tồn tại một số nhóm đối tượng có thể có được mật mã, đó là: bộ phận cung cấp phần mềm; bộ phận cài đặt phần mềm, những người có thể sử dụng máy tính có cài đặt phần mềm. Ngoài ra, mật mã có thể bị đánh cắp. Cũng có thể, chủ nhân chữ ký số chuyển giao cho người khác mật mã của mình. Như vậy, tính bảo mật của chữ ký số không phải là tuyệt đối.

- Vấn đề bản gốc, bản chính: Nếu đối với tài liệu giấy, chữ ký được ký một lần và chỉ có một bản duy nhất (được coi là bản gốc). Bản gốc được ký bằng chữ ký sẽ không thể cùng lúc ở hai chỗ khác nhau. Có thể tin tưởng rằng, nếu bản gốc duy nhất mất đi thì sẽ không thể có bản thứ hai giống hệt như vậy.

Nhưng với văn bản điện tử đã được ký bằng chữ ký số, người ta có thể copy lại và bản copy từ bản chính và bản copy từ bản copy không có gì khác biệt so với bản chính duy nhất được ký. Đây là một thách thức đối với công tác văn bản và cả nền hành chính. Khái niệm bản gốc, bản chính trong văn bản hành chính sẽ phải xem xét lại đối với văn bản điện tử.

- Sự có thời hạn của chữ ký điện tử. Chữ ký điện tử là chương trình phần mềm được cấp có thời hạn cho người sử dụng. Về lý thuyết, văn bản sẽ có hiệu lực pháp lý khi được ký trong thời hạn sử dụng của chữ ký.

Tuy nhiên, thực tế hiệu lực pháp lý của văn bản hoàn toàn có thể bị nghi ngờ khi chữ ký số hết thời hạn sử dụng. Đây cũng là một hạn chế và thách thức rất lớn đối với việc sử dụng chữ ký số.

- Thời gian xử lý chậm vì phải thực hiện việc mã hóa và giải mã của hàm băm SHA-1.

3.3. THIẾT KẾ PHẦN MỀM

Chương trình được chia làm 2 quá trình: Quá trình mã hóa và gửi tệp tin đi được thực hiện bởi người gửi và quá trình nhận tệp tin và giải mã so khớp chữ ký được thực hiện bởi người nhận.

- Quá trình mã hóa và gửi tệp tin:

Bước 1: Người gửi thiết đặt giá trị khóa bí mật và khóa công khai của mình, đồng thời nhập giá trị khóa công khai của người nhận.

Bước 2: Chọn tệp tin cần gửi đi và tiến hành băm tệp tin theo thuật toán SHA-1 được giá trị băm là C.

Bước 3: Tiến hành ký số và mã hóa C ta được bản mã D và chữ ký K.

Bước 4: Đính kèm D và K vào tệp tin và gửi tệp tin

- Quá trình giải mã và so khớp chữ ký

Bước 1: Người nhận nhận tệp tin và tiến hành tách D, K ra khỏi tệp tin

Bước 2: Nhập giá trị khóa bí mật và khóa công khai cho chương trình

Bước 3: Giải mã D và K tiến hành so khớp chữ ký, nếu khớp thì đưa ra được giá trị băm C, ngược lại thông báo giá trị băm đã bị thay đổi dừng chương trình

Bước 4: Tiến hành băm tệp tin đã nhận theo thuật toán SHA-1 được giá trị băm C', so sánh C' với C. Nếu C'=C thì tệp tin được bảo toán ngược lại thông báo tệp tin đã bị thay đổi.

3.4. GIAO DIỆN CHƯƠNG TRÌNH

Giao diện chính của chương trình gồm các nút lệnh sau:

1. Nút "Chọn file" dùng để chọn một tệp tin mà người dùng muốn gửi đi.

2. Nút "SHA-1" dùng để tự động tính ra bảng băm SHA-1 của file người dùng vừa chọn.

3. Nút "Mã hóa" là nút khi nhấn sẽ đưa ra bảng nhập khóa.

4. Nút "Tạo khóa" dùng để tạo khóa bí mật và khóa công khai cho người dùng, với chức năng này hệ thống sẽ yêu cầu người dùng thiết lập 2 giá trị p, q là 2 số nguyên tố để phục vụ cho quá trình sinh khóa

5. Nút "Ngẫu nhiên" dùng để tự động sinh khóa bí mật và khóa công khai cho người dùng một cách ngẫu nhiên cho người dùng.

6. Nút “Submit” là nút xác nhận khóa và tiến hành tính toán.

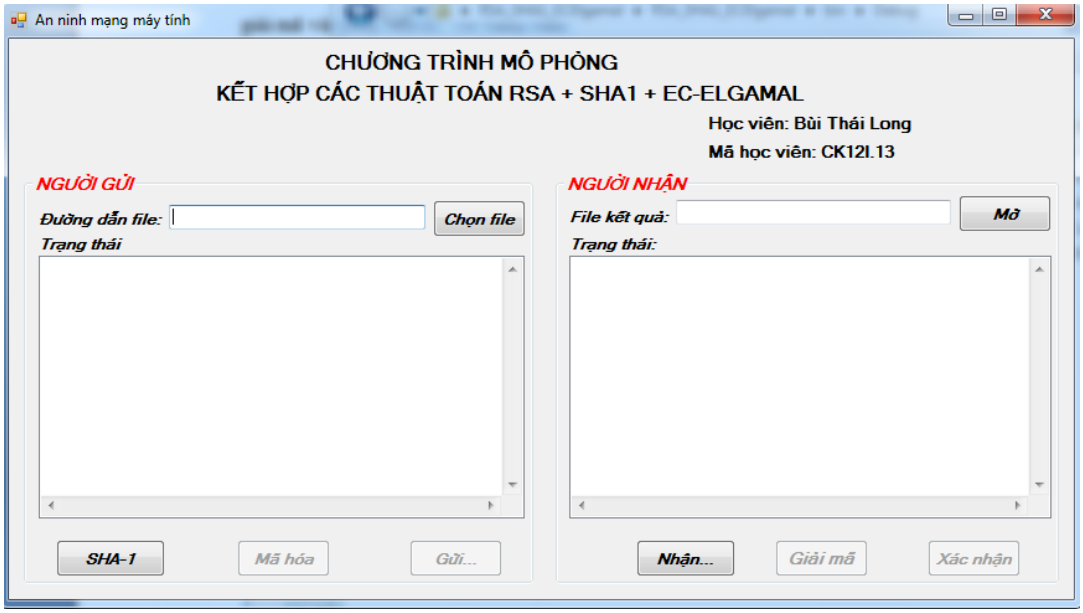
7. Nút “Gửi..” dùng để gửi tệp tin cùng với bản băm và chữ ký dưới dạng mã hóa cho người nhận

8. Nút “Nhận…” người nhận sử dụng nút này để tiến hành nhận dữ liệu từ người gửi, khi nhận đủ thông tin hệ thống sẽ thông báo hoàn thành.

9. Nút “Giải mã” hệ thống sẽ căn cứ vào các khóa do người nhận cấp để tiến hành giải mã và khớp chữ ký với bảng băm.

10. Nút “Xác nhận” sau khi giải mã và khớp thành công chương trình sẽ so sánh bảng băm SHA-1 vừa giải mã được với bảng băm SHA-1 của tệp tin vừa nhận được, nếu 2 bảng băm này như nhau thì kết luận tệp tin vừa nhận đúng của người gửi và quá trình truyền tin là an toàn, ngược lại sẽ kết luận tệp tin đã bị sửa đổi.

3.4.1. Giao diện chương trình.



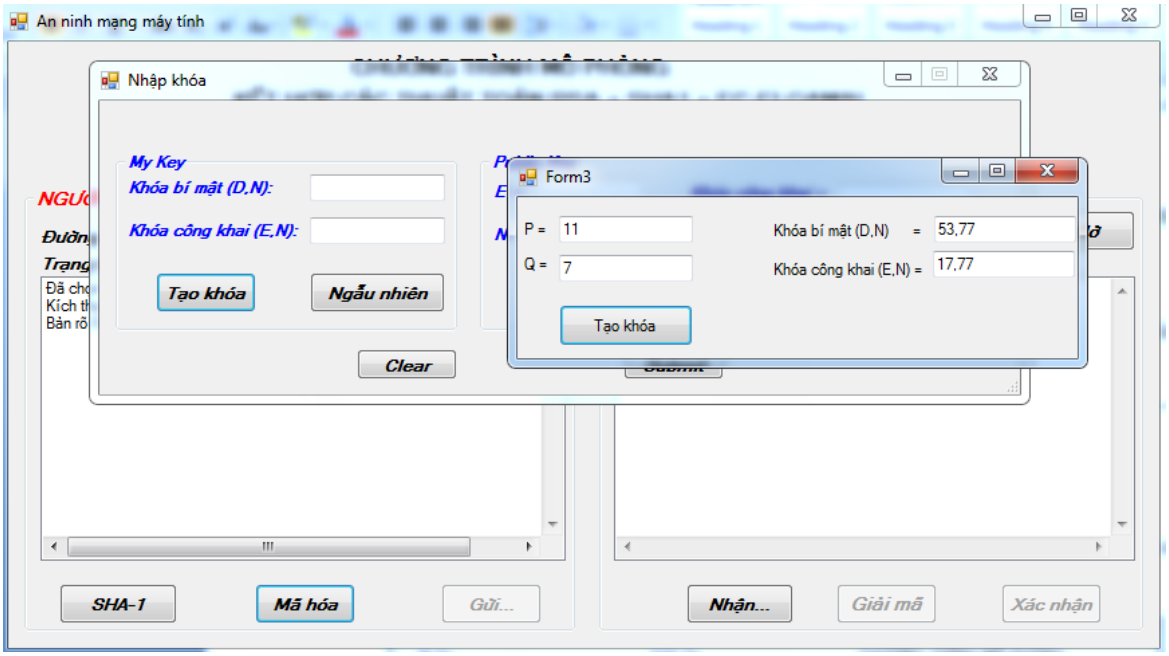
Hình 3.4. Giao diện chương trình chính

1./ Quá trình băm file sử dụng SHA-1.

Người gửi chọn file cần gửi sau đó nhấn SHA-1. Chương trình đưa ra bảng rõ SHA-1.

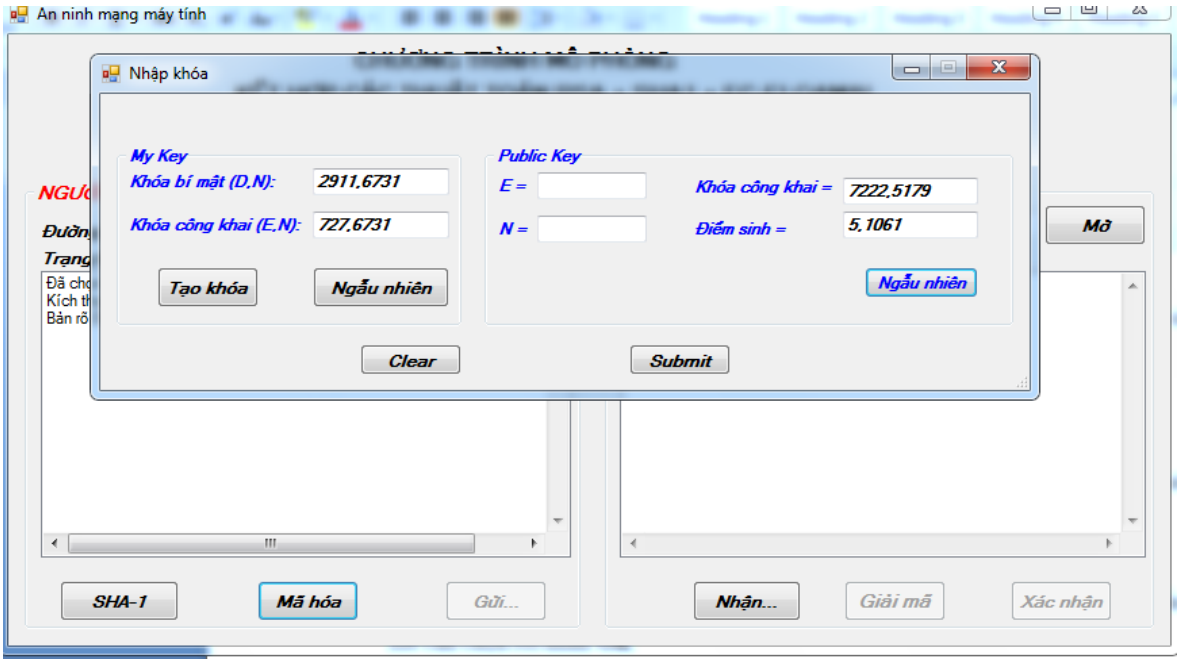
Người gửi tiến hành mã hóa bằng nút “Mã hóa”.

- ***Cách 1***: Dùng nút ***Tạo khóa*** sau đó lựa chọn các giá trị P, Q thích hợp (P, Q là các số nguyên tố. Sau đó nhấn nút tạo khóa để được khóa bí mật và khóa công khai)



Hình 3.5. Giao diện tạo khóa bằng nút *Tạo khóa*

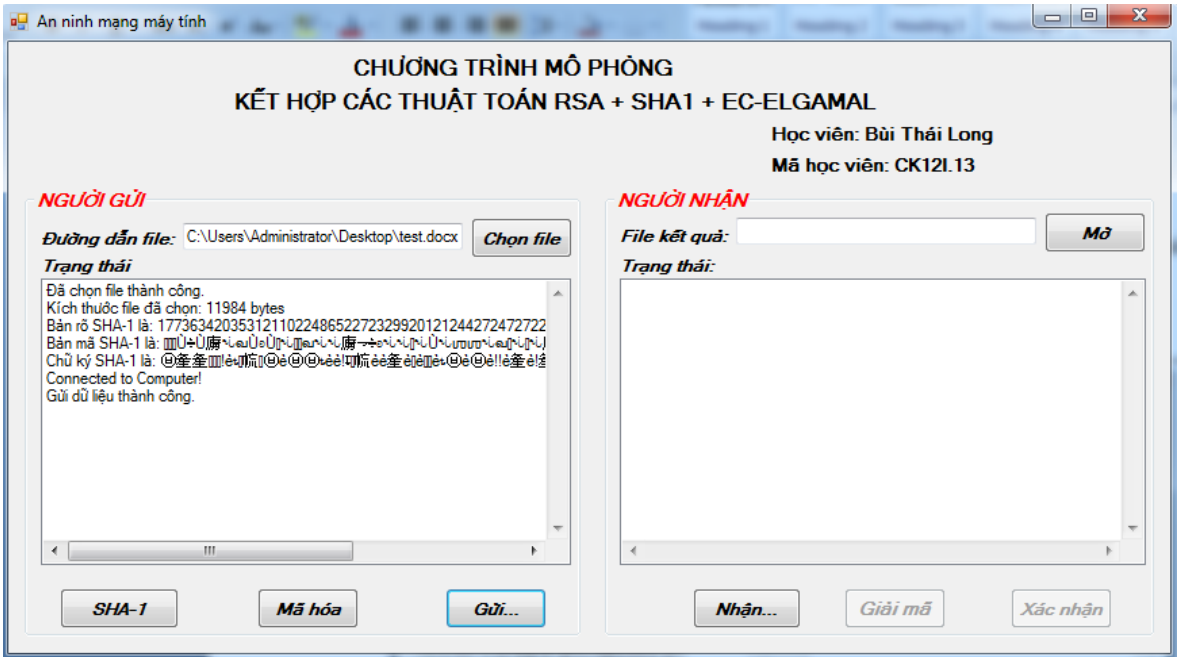
- ***Cách 2***: Dùng nút tạo ***Ngẫu nhiên*** để chương trình tự sinh ra khóa công khai và khóa bí mật, điểm sinh



Hình 3.6. Giao diện tạo khóa bằng nút *Ngẫu nhiên*

Sau đó người gửi và người nhận chuyển mã công khai cho nhau nhập các giá trị **E**, **N** vào ***Public Key.*** Rồi chọn ***Submit.*** Chương trình sẽ tiến hành mã hóa.

2./ Quá trình của người gửi.



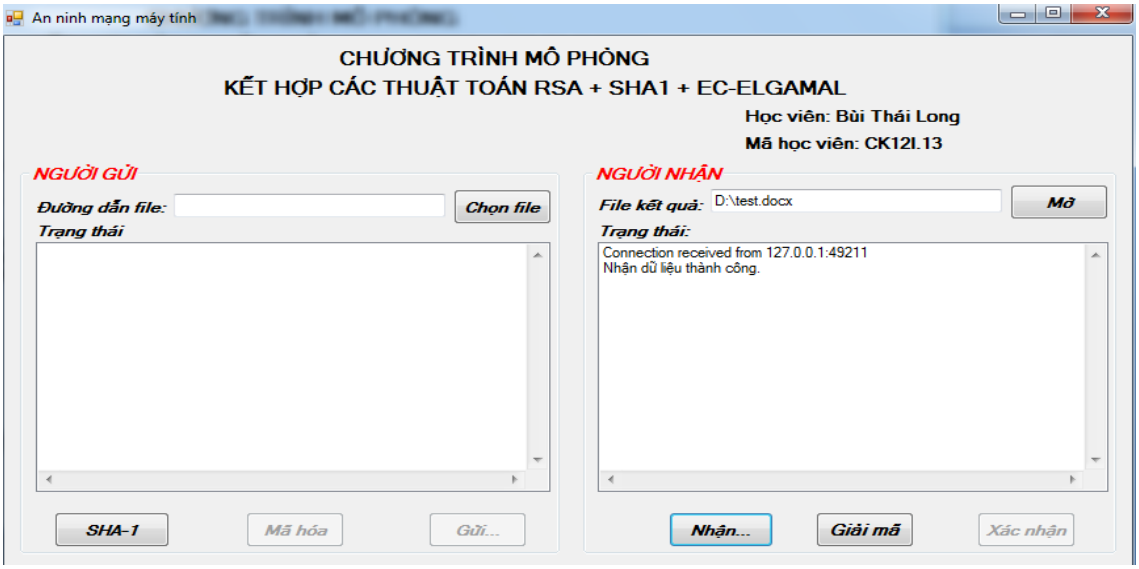
Hình 3.7. Giao diện quá trình mã hóa

- Khi đã mã hóa thành công nhấn nút Gửi… để gửi đến cho người nhận. Quá trình mã hóa và gửi file của người gửi kết thúc.

3./ Quá trình của người nhận

+ Quá trình nhận dữ liệu

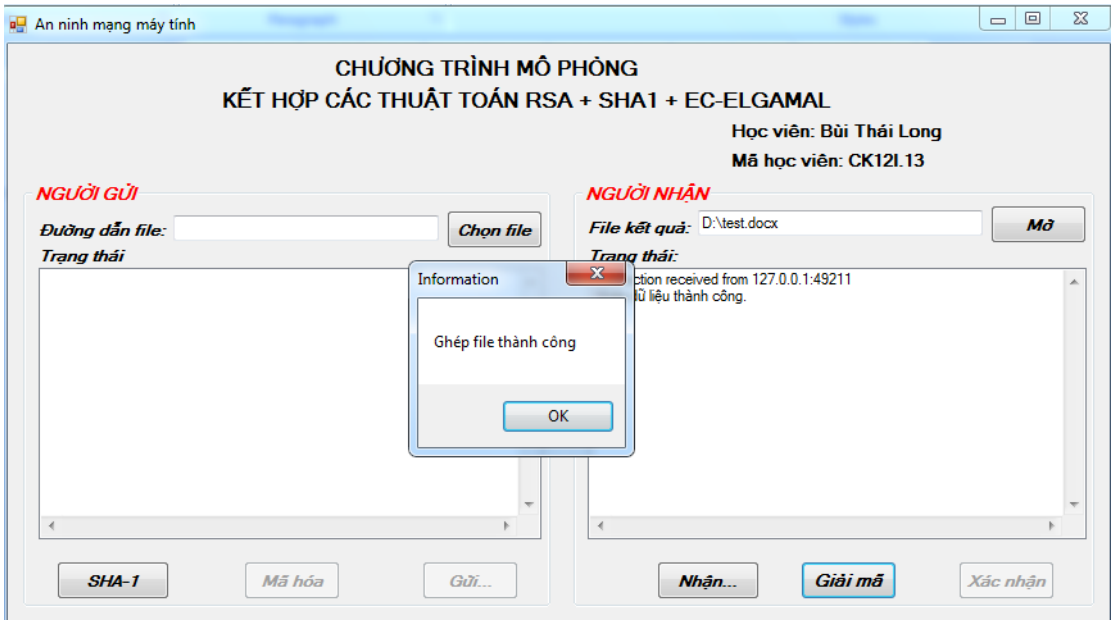
Người nhận tiến hành nhận dữ liệu bằng nút ***Nhận..*** và được thông báo nhận dữ liệu thành công



Hình 3.8. Giao diện quá trình nhận dữ liệu

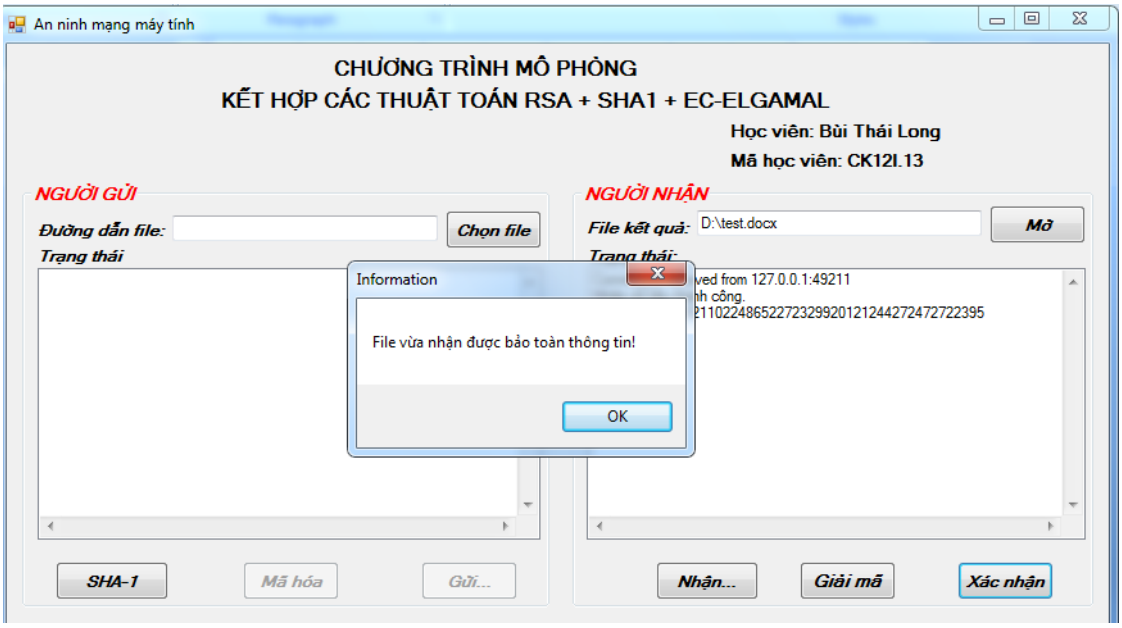
+ Quá trình giải mã dữ liệu

- Sau khi nhận dữ liệu thành công ta tiến hành giải mã bằng nút "***Giải mã***" và nhận được quá trình ghép file thành công.



Hình 3.9. Giao diện giải mã dữ liệu

- Khi ghép file thành công ta tiến hành xác nhận file xem có được bảo toàn hay không bằng nút "***Xác nhận***". Sẽ có bảng thông báo nhập lại khóa công khai và khóa bí mật của người nhận và khóa công khai của người gửi. Nhập xong nhấn nút "***Submit***" để chương trình xác nhận.



Hình 3.10. Giao diện xác nhận dữ liệu

- Để xem file vừa nhận được ta nhấn nút ***Mở*** để mở đường dẫn chứa file do bên người gửi gửi đến.

3.4.2. Kết quả

Kết quả của chương trình thu được là file mà bên người gửi đã gửi được bảo toàn thông tin. Và trên hết là quá trình gửi của file được bảo toàn trên đường truyền. Không bị sai lệch thông tin của file đã nhận.

3.5. ĐÁNH GIÁ

- Hệ mã hóa RSA + SHA-1 + EC-Elgamal đã giải quyết được yêu cầu của bài toán khá tốt. Có thể được áp dụng trong các bài toán như trao đổi dữ liệu điện tử, thương mại điện tử, chuyển đổi tiền tệ, … Nhưng về tốc độ thì giải thuật này còn chậm .

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN ĐỀ TÀI

❖ Kết luận

Sau một thời gian nghiên cứu và tìm hiểu luận văn "***Nghiên cứu một số phương pháp bảo đảm an toàn thông tin trong mạng máy tính***" đã đạt được một số kết quả như sau:

- Nghiên cứu về các vấn đề trên mạng máy tính, dạng tấn công và hiểm họa trên mạng máy tính

- Nghiên cứu một số phương pháp bảo vệ thông tin trên mạng như dùng tưởng lửa, dùng công nghệ mã hóa, dùng mạng riêng ảo, …trong đó đi sâu nghiên cứu về phương pháp dùng công nghệ mã hóa.

- Nghiên cứu thuật toán mã hóa RSA và chữ ký số, kết hợp hàm băm SHA-1, EC-Elgamal vào trong quá trình mã hóa và giải mã để xác minh tính toàn vẹn của dữ liệu.

- Cài đặt thử nghiệm thuật toán mã hóa RSA + SHA-1.

- Cài đặt thử nghiệm thuật toán mã hóa RSA + SHA-1 + EC-Elgamal

❖ Hạn chế

Về chương trình ứng dụng: do thời gian có hạn nên tôi chưa có điều kiện xây dựng một phần mềm ứng dụng hoàn chỉnh, áp dụng các thuật toán trên vào thực tế.

❖ Hướng phát triển

Với việc nghiên cứu một số phương pháp đảm bảo an toàn thông tin trong mạng thông tin, tôi sẽ nghiên cứu sâu hơn về hướng này và sẽ áp dụng vào các bài toán thực tế như bảo mật trao đổi dữ liệu điện tử, thương mại điện tử, email, chat, winword, …

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] GS. Phạm Đình Diệu (2006), *Lý thuyết mật mã và an toàn thông tin*, nhà xuất bản Đại học Quốc gia Hà Nội.

[2] Nguyễn Xuân Dũng (2007), *Bảo mật thông tin mô hình và ứng dụng*, NXB Thống kê.

[3] Trịnh Nhật Tiến, (2008) *Giáo trình an toàn dữ liệu và mã hóa*, Đại học Công nghệ - Đại học Quốc Gia Hà Nội,

[4] Phan Huy Khánh, Hồ Phan Hiếu, Trường Đại học Bách khoa, Đại học Đà Nẵng. (2009) *Giải pháp ứng dụng chữ ký điện tử trong quá trình nhận và gửi văn bản*, Tạp chí khoa học và công nghệ, Đại học Đà Nẵng – số 5(34)..

[5] Viện Công nghệ Thông Tin (2000), *Nghiên cứu tiếp cận một số vần đề hiện đại của mạng thông tin máy tính*, Báo cáo kết quả nghiên cứu khoa học công nghệ.

Tiếng Anh

[6] Andrew S. Tanenbaum (1988), *Computer Networks, Second Edition*, Prentice – Hall International.

[7] An Elliptic Curve Based Homomorphic Remote Voting System, 2014

[8] An elecronic voting platform with elliptic curve cryptography, 2011

[9] Douglas E. Comer (1995), *Internetworking with TCP/IP, Volume I, Principles, Protocols and Architecture*, Third Edition, Prentice - Hall International.

[10] Fred Halsall (1992), *Data Communications, Computer Networks and Open Systems*, Third Edition, Addison – Wesley Publishing Company.

[11] Securing E-voting with EC-ElGamal, 2010

[12] Chris Hare and Karanjit Siyan (1996), *Internet Firewalls and Network Security*, New Riders Publishing, Indianopolis, Indiana.

[13] Các website:

http://www.cryptography.com

http://www.vi.wikipedia.org/wiki/Digital_signature