BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP

NGÀNH : CÔNG NGHỆ THÔNG TIN

Sinh viên thực hiện : Phạm Duy Tuấn Thịnh

Giảng viên hướng dẫn: TS. Hồ Văn Canh

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

TÌM HIỂU VỀ HÀM BĂM RIPEMD VÀ ỨNG DỤNG TRONG CHỮ KÝ SỐ

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

NGÀNH: Công Nghệ Thông Tin

Sinh viên thực hiện : Phạm Duy Tuấn Thịnh

Giảng viên hướng dẫn: TS. Hồ Văn Canh

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên: **Phạm Duy Tuấn Thịnh** **Mã SV**: **1512101013**

Lớp : **CT1910M**

Ngành : **Công Nghệ Thông Tin**

Tên đề tài: **Tìm hiểu về hàm băm Ripemd và ứng dụng trong chữ ký số**

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

a. Nội Dung :

- Khảo sát thực trạng về an ninh mạng máy tính tại Việt nam.
- Tìm hiểu các lỗ hổng bảo mật mạng máy tính.
- Một số kỹ thuật phổ biến phòng và phát hiện xâm nhập mạng máy tính.

b. Các yêu cầu cần giải quyết :

- Tìm hiểu thực trạng về an ninh mạng máy tính tại Việt Nam.
- Tìm hiểu các lỗ hổng bảo mật mạng máy tính.
- Tìm hiểu một số kỹ thuật phổ biến phòng và phát hiện xâm nhập mạng máy tính.

2. Các tài liệu, số liệu cần thiết

……

……

3. Địa điểm thực tập tốt nghiệp

…….

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Họ và tên : **Hồ Văn Canh**

Học hàm, học vị : **Đại tá, Tiến sĩ.**

Cơ quan công tác : **Cục KTNV-BCA**

Nội dung hướng dẫn:

- Khảo sát thực trạng về an ninh mạng máy tính tại Việt nam.
- Tìm hiểu các lỗ hổng bảo mật mạng máy tính.
- Một số kỹ thuật phổ biến phòng và phát hiện xâm nhập mạng máy tính.

Đề tài tốt nghiệp được giao ngày 1 tháng 8 năm 2022

Yêu cầu phải hoàn thành xong trước ngày 22 tháng 10 năm 2022

Đã nhận nhiệm vụ ĐTTN	Đã giao nhiệm vụ ĐTTN
Sinh viên	*Giảng viên hướng dẫn*
Phạm Duy Tuấn Thịnh	**Hồ Văn Canh**

Hải Phòng, ngày ….. tháng….. năm 2022

TRƯỞNG KHOA

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN TỐT NGHIỆP

Họ và tên giảng viên:

.....

Đơn vị công tác:

.....

Họ và tên sinh viên : ..... Ngành: Công nghệ Thông tin

Nội dung hướng dẫn:

.....

1.Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp

.....

.....

.....

.....

.....

.....

2.Đánh giá chất lượng của đồ án/khóa luận (so với nội dung yêu cầu đã đề ra trong nhiệm vụ Đ.T. T.N trên các mặt lý luận, thực tiễn, tính toán số liệu…)

.....

.....

.....

.....

.....

.....

3. Ý kiến của giảng viên hướng dẫn tốt nghiệp

Đạt ☐ Không đạt ☐ Điểm:……...

Hải Phòng, ngày .... tháng ..... năm 2022

Giảng viên hướng dẫn

(Ký và ghi rõ họ tên)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN CHẤM PHẢN BIỆN

Họ và tên giảng viên:
.....
Đơn vị công tác:
.....
Họ và tên sinh viên:
..... Ngành: Công nghệ thông tin
Đề tài tốt nghiệp:
.....

1. Phần nhận xét của giảng viên chấm phản biện

.....
.....
.....
.....
.....
.....
.....

2. Những mặt còn hạn chế

.....
.....
.....
.....
.....
.....
.....

3. Ý kiến của giảng viên chấm phản biện

Được bảo vệ ☐ Không được bảo vệ ☐ Điểm:

Hải Phòng, ngày …… tháng ….. năm 2022

Giảng viên chấm phản biện

(Ký và ghi rõ họ tên)

LỜI CẢM ƠN

Để hoàn thành tốt đề tài này em xin chân thành cảm ơn ban lãnh đạo Trường Đại Học Quản Lý Và Công Nghệ Hải Phòng cùng tất cả các giảng viên đã tạo điều kiện thuận lợi và nhiệt tình giảng dạy cho em trong suốt thời gian học vừa qua để em có thể học tập tốt và đạt được kết quả như ngày hôm nay.

Em cũng xin chân thành gửi lời cảm ơn đến T.S Hồ Văn Canh đã tận tình hướng dẫn cho em về đề tài và đồng thời em cũng xin gửi lời cảm ơn đến các bạn thành viên ở một số webiste và diễn đàn đã cung cấp thêm một số thống tin hữu ích cho em thực hiện tốt đề tài này.

Do quy mô đề tài, thời gian và kiến thức còn hạn chế nên không tránh khỏi những sai sót. Kính mong quý thầy cô đóng góp ý kiến để em củng cố, bổ sung và hoàn thiện thêm kiến thức cho mình.

Hải Phòng, ngày 22 tháng 10 năm 2022

Sinh Viên

Phạm Duy Tuấn Thịnh

MỤC LỤC

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Ngày nay, khi Internet đã phát triển phổ biến rộng rãi, các tổ chức, cá nhân đều có nhu cầu giới thiệu thông tin của mình trên xa lộ thông tin cũng như thực hiện các phiên giao dịch trực tuyến một cách tiện lợi nhất. Vấn đề nảy sinh là khi phạm vi ứng dụng của các ứng dụng trên internet ngày càng mở rộng thì khả năng xuất hiện lỗi càng cao. Từ đó nảy sinh ra các vấn đề về hệ thống mạng không đáng có xảy ra gây ảnh hưởng đến xã hội, kinh tế … Những lỗi này hầu như do người làm không kiểm duyệt kĩ lưỡng trước khi đưa cho người dùng cuối hay cũng có thể do có người cố tình phá hoại nhằm đánh cắp thông tin cá nhân như tài khoản ngân hàng, điện thoại, tin nhắn, …

Điều này cho thấy hình thái chiến tranh thông tin đã và đang dần dần hình thành ở Việt Nam. Vấn đề an toàn thông tin cho mạng máy tính và việc nghiên cứu về chiến tranh thông tin trên mạng và giải pháp phòng tránh, đánh trả cụ thể là một nhu cầu cấp bách hiện nay. Chính vì vậy em đã chọn đồ án tốt nghiệp : “ Tìm hiểu về hàm băm Ripemd và ứng dụng trong chữ ký số ”.

Đồ án gồm ba chương:

- Khảo sát thực trạng về an ninh mạng máy tính tại Việt nam.
- Tìm hiểu các lỗ hổng bảo mật mạng máy tính.
- Một số kỹ thuật phổ biến phòng và phát hiện xâm nhập mạng máy tính.

CHƯƠNG 1: KHẢO SÁT THỰC TRẠNG VỀ AN NINH MẠNG MÁY TÍNH TẠI VIỆT NAM

1.1 Thực trạng an ninh mạng tại Việt Nam :

Internet ngày càng phát triển mạnh mẽ và có sức ảnh hưởng rộng rãi tới tất cả các ngành nghề, các lĩnh vực của cuộc sống. Hiện nay, Internet đã trở thành một môi trường phức tạp, bao hàm mọi thành phần xã hội. Con người sử dụng Internet với nhiều mục đích khác nhau, trong đó có một số người tận dụng khả năng truyền bá thông tin nhanh chóng để phát tán những tin tức, sự kiện với mục đích làm phương hại đến tên tuổi, uy tin của một cá nhân, tổ chức hay đến sự ổn định một quốc gia nhằm mục đích chính trị.

Phần lớn các cuộc tấn công trên mạng được thực hiện thông qua việc sử dụng một hoặc nhiều công cụ phần mềm (do người tấn công tự xây dựng hoặc có được từ các nguồn khác nhau . Trong bản luận văn này, những phần mềm đó được gọi là các phần mềm phá hoại.

Phần mềm phá hoại là những phần mềm được thiết kế, xây nhựng nhằm mục đích tấn công gây tổn thất hay chiếm dụng bất hợp pháp tài nguyên của máy tính mục tiêu (máy tính bị tấn công . Những phần mềm này thường được che dấu hay hoá trang như là phần mềm hợp lệ, công khai hoặc bí mật thâm nhập vào máy tính mục tiêu.

Những phần mềm phá hoại khác nhau có phương thức và nguy cơ gây hại khác nhau.

Các vụ tấn công trên mạng ngày càng gia tăng cả về qui mô và tính chất nguy hiểm. Có thể kể ra một số vụ tấn công như sau:

Tình hình an ninh mạng 2019:

Theo kết quả đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện, trong năm 2019, chỉ tính riêng thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 20.892 tỷ đồng (tương đương 902 triệu USD), hơn 1,8 triệu máy tính bị

mất dữ liệu do sự lan tràn của các loại mã độc mã hóa dữ liệu tống tiền (ransomware), trong đó có nhiều máy chủ chứa dữ liệu của các cơ quan, gây đình trệ hoạt động của nhiều cơ quan, doanh nghiệp.

Phân tích về những nguyên nhân dẫn tới số lượng máy tính bị nhiễm virus ở mức cao, các chuyên gia Bkav cho biết nguyên nhân đầu tiên là việc tải và cài đặt các phần mềm không rõ nguồn gốc, trôi nổi trên mạng. Trung bình, cứ 10 máy tính cài các phần mềm tải về từ Internet thì có tới 8 máy tính sẽ bị nhiễm viurs, đây là một tỷ lệ rất cao. Để đảm bảo an toàn, người sử dụng chỉ nên tải các phần mềm có nguồn gốc rõ ràng, từ nhà sản xuất tin tưởng và từ các kho ứng dụng chính thống, không tải từ những nguồn trôi nổi trên mạng.

Năm 2019, tiếp tục chứng kiến sự hoành hành của các loại mã độc mã hóa dữ liệu tống tiền (ransomware). Theo thống kê của Bkav, số lượng máy tính bị mất dữ liệu trong năm 2019 lên tới 1,8 triệu lượt, tăng 12% so với năm 2018. Nghiêm trọng hơn, trong số này có rất nhiều máy chủ (server) chứa dữ liệu của các cơ quan. Không chỉ gây thiệt hại lớn, việc các máy chủ bị xóa dữ liệu cũng gây đình trệ hoạt động của cơ quan, doanh nghiệp trong nhiều ngày sau đó, thậm chí đến cả tháng.

420.000 máy tính tại Việt Nam đã bị nhiễm loại mã độc tấn công APT nguy hiểm W32.Fileless. Theo các chuyên gia Bkav, kỹ thuật mà W32.Fileless sử dụng rất tinh vi và có thể nói đã đạt đến mức "tàng hình". Mã độc này không để lại bất cứ dấu hiệu gì về sự tồn tại của chúng dưới dạng file nhị phân trên ổ cứng máy tính như các loại mã độc thông thường.

Do khả năng ẩn giấu gần như trong suốt với người dùng, mã độc này sẽ nằm vùng, đánh cắp thông tin, mở cổng hậu để tin tặc có thể chiếm quyền điều khiển máy tính từ xa. Bkav cũng ghi nhận một số dòng W32.Fileless có tải về thêm các mã độc khác để lợi dụng tài nguyên máy tính đào tiền ảo.

Tình hình an ninh mạng 2020:

Năm 2020, COVID-19 bùng phát, hàng loạt doanh nghiệp, cơ quan, tổ chức chuyển sang làm việc từ xa. Các phần mềm làm việc trực tuyến được tìm kiếm và download rầm rộ. Nhiều đơn vị buộc phải mở hệ thống ra Internet để nhân viên có thể truy cập và làm việc từ xa… Điều này tạo môi trường cho kẻ xấu khai thác lỗ hổng, tấn công, đánh cắp thông tin.

Trong năm 2020, hàng loạt vụ tấn công mạng quy mô lớn diễn ra trên toàn cầu, điển hình như vụ việc nhà máy của Foxconn bị tin tặc tấn công, bị đòi 34 triệu USD tiền chuộc dữ liệu; hay 267 triệu thông tin người dùng Facebook được rao bán; Intel bị tin tặc tấn công, gây rò rỉ 20GB dữ liệu bí mật… Mới đây nhất, T-Mobile, một trong những nhà mạng lớn nhất của Mỹ cũng đã trở thành nạn nhân tiếp theo của hacker. Theo quan sát của Bkav, tại Việt Nam, nhiều trang thương mại điện tử lớn, một số nền tảng giao hàng trực tuyến có nhiều người sử dụng, đã bị xâm nhập và đánh cắp dữ liệu.

Chỉ tính riêng năm 2020, hàng trăm tỷ đồng đã bị hacker chiếm đoạt qua tấn công an ninh mạng liên quan đến ngân hàng, trong đó chủ yếu là các vụ đánh cắp mã OTP giao dịch của người dùng. Cách thức chính của hacker là lừa người dùng cài đặt phần mềm gián điệp trên điện thoại để lấy trộm tin nhắn OTP, thực hiện giao dịch bất hợp pháp. Trung bình mỗi tháng, hệ thống giám sát virus của Bkav đã phát hiện hơn 15.000 phần mềm gián điệp trên điện thoại di động. Điển hình là vụ việc VN84App, phần mềm thu thập tin nhắn OTP giao dịch ngân hàng lên đến hàng tỷ đồng, đã lây nhiễm hàng nghìn smartphone tại Việt Nam.

Hình thức tấn công có chủ đích APT sử dụng mã độc tàng hình đã thực sự bùng phát trong năm 2020. Theo thống kê của Bkav, đã có ít nhất 800.000 máy tính tại Việt Nam bị nhiễm loại mã độc này trong năm 2020, tăng gấp đôi so với năm 2019.

Mã độc tàng hình Fileless là loại mã độc đặc biệt, không có file nhị phân trên ổ cứng máy tính như các loại mã độc thông thường. Kỹ thuật này giúp Fileless dễ dàng

qua mặt hầu hết các phần mềm diệt virus trên thị trường bởi các phần mềm này chỉ phát hiện virus qua mẫu nhận diện.

Tình hình an ninh mạng 2021:

70,7 triệu lượt máy tính bị nhiễm virus trong năm 2021, báo động đỏ cho tình hình an ninh mạng tại Việt Nam. Trong những năm gần đây, Việt Nam luôn là một trong những quốc gia có tỷ lệ nhiễm mã độc và hứng chịu các cuộc tấn công mạng thuộc nhóm cao trên thế giới. Không những thế, mức độ sử dụng máy tính và các thiết bị thông minh tại Việt Nam đã tăng đột biến bởi ảnh hưởng của COVID-19, đây chính là môi trường lý tưởng để virus bùng phát và lây lan mạnh.

Tại Việt Nam, số lượt máy tính bị virus mã hoá dữ liệu tấn công trong năm 2021 lên tới hơn 2,5 triệu lượt, cao gấp 4,5 lần so với năm 2020. Đa số người sử dụng Việt Nam vẫn còn lúng túng, chưa biết cách ứng phó khi máy tính bị mã hoá dữ liệu. Hơn 99% người tham gia chương trình Đánh giá an ninh mạng 2021 của Bkav chọn làm theo hướng dẫn trả tiền với hy vọng lấy lại được dữ liệu của mình từ hacker. Cách làm này không những bạn có thể không lấy lại được dữ liệu mà còn mất tiền oan. Cần phòng vệ một cách chủ động, thiết lập các biện pháp bảo vệ an toàn cho dữ liệu, đặc biệt cần có cơ chế sao lưu dữ liệu định kỳ.

Sau 2 năm chuyển dịch từ Zero COVID sang thích ứng an toàn, việc học tập, làm việc, mua sắm, thậm chí du lịch, giải trí… đều theo hình thức online đã trở thành những kỹ năng quen thuộc đối với mỗi người. Theo báo cáo đánh giá an ninh mạng của Bkav, nhận thức bảo đảm an toàn an ninh thông tin của người dùng đã được cải thiện đáng kể.

Tuy nhiên, còn một kỹ năng quan trọng nhưng lại đang bị người dùng bỏ qua là kiểm tra đường link của website có sử dụng HTTPS hay không trước khi thực hiện giao dịch. HTTPS giống như một “tick xanh” đánh dấu những website an toàn, đã được đăng ký chính chủ. Đa số các website hiện nay đều cung cấp HTTPS và giao thức này

trở thành tiêu chuẩn gần như bắt buộc cho tất cả website có thực hiện giao dịch ngân hàng, mua sắm. Đáng tiếc, chỉ có 30% người dùng biết về giao thức HTTPS; số còn lại vẫn chấp nhận dùng HTTP mà không hay biết về nguy cơ bị tấn công giả mạo. Để tránh nguy cơ bị tấn công, người dùng tuyệt đối không giao dịch quan trọng trên các website bắt đầu bằng HTTP.

1.2 Khái niệm "Chiến tranh thông tin" :

Cùng với sự phát triển mạnh mẽ của công nghệ thông tin, sự bùng nổ thông tin là sự hình thành của loại hình chiến tranh mới – Chiến tranh thông tin. Không dùng súng đạn, vũ khí hạt nhân,… để tấn công, Internet sử dụng một công cụ cực kỳ hữu dụng để tấn công đối phương. Các thế lực thù địch lợi dụng sự phát triển của Internet, lợi dụng tự do ngôn luận để tấn công đối phương trên lĩnh vực thông tin, làm sai lệch thông tin, bóp m o sự thật về thông tin của đối phương, thậm trí làm tê liệt các hệ thống thông tin của đối phương. Đặc biệt các thế lực thù địch còn sử dụng các hacker chuyên nghiệp tập trung tấn công vào cơ sở hạ tầng thông tin của đối phương thuộc các lĩnh vực như: quân sự, tài chính, ngân hàng, mạng máy tính quốc gia,… sử dụng Virus để làm cho hệ thống vũ khí của đối phương bị mất điều khiển, phá hoại cơ sở hạ tầng kinh tế quốc dân làm cho nền kinh tế của đối phương bị rối loạn,… hay đánh cắp những bí mật quân sự, những thông tin quốc gia quan trọng của đối phương.

Tại Việt Nam, loại hình chiến tranh thông tin ngày càng được hình thành rõ. Trong thời gian gần đây, các thế lực thù địch đã lợi dụng mạng Internet để lập các website cá nhân, sử dụng các mạng xã hội đưa những thông tin sai lệch không đúng sự thật về Đảng về Nhà nước lên mạng nhằm bôi xấu, gây mất lòng tin của nhân dân với Đảng và Nhà nước ta. Hàng loạt các website của Việt Nam bị các hacker nước ngoài tấn công làm tê liệt trong một thời gian. Thậm trí có những website Việt Nam bị tấn công còn để lại những hình ảnh và những dòng chữ Trung Quốc.

Với xu hướng toàn cầu hoá hiện nay, các mạng lưới truyền thông và xử lý thông tin của các Quốc gia được liên kết với nhau. Do đó ở đâu có điểm kết nối mạng thì ở

đó đều có thể xảy ra chiến tranh thông tin. Do vậy các quốc gia cần phải có biện pháp xây dựng các lớp bảo vệ hệ thống thông tin của mình, đồng thời cũng phải chuẩn bị các phương án tấn công các hệ thông tin của đối phương.

CHƯƠNG 2: CÁC LỖ HỔNG BẢO MẬT MẠNG MÁY TÍNH

2.1 Khái niệm lỗ hổng :

Lỗ hổng bảo mật là khuyết điểm trong quá trình lập trình hoặc việc cấu hình sai hệ thống mà qua đó tạo ra sơ hở dẫn đến kẻ tấn công mạng có thể truy cập trực tiếp dữ liệu mà bỏ qua quy trình thông thường.

Lỗ hổng bảo mật có thể xảy ra ở tất cả các lớp bảo mật bao gồm: cơ sở hạ tầng, mạng và ứng dụng (application).

Hệ điều hành Microsoft Windows có nguồn gốc phát triển cho các máy tính cá nhân và các mạng an toàn, tuy nhiên nó lại không an toàn đối với mạng phi chính phủ như Internet.

Trong giai đoạn ban đầu, Microsoft thiết kế hệ điều hành Microsoft Windows mà chưa nghĩ tới tầm quan trọng của Internet khi gắn liền với nó. Điều đó đã dẫn tới một số điểm yếu là các lỗ hổng bảo mật.

Một lỗ hổng bảo mật cho phép một người nào đó xâm nhập vào máy tính của bạn qua đường kết nối Internet. Những lỗ hổng nhỏ có thể chỉ cho phép truy cập vào clipboard của bạn, nhưng những lỗ hổng lớn có thể cho phép họ tiếp quản hoàn toàn máy tính của bạn.

Như vậy, lỗ hổng bảo mật là một trong những nguyên nhân dẫn đến sự mất an toàn của các hệ thống máy tính khi kết nối Internet.

Để thực hiện cơ chế an toàn, các hệ điều hành (hoặc các Website phải được thiết kế để đáp ứng các yêu cầu về mặt an toàn đặt ra. Tuy nhiên, trên thực tế, việc thiết kế các hệ điều hành (hoặc các Website chỉ đạt đến mức độ tiếp cận các yêu cầu an toàn chứ không đáp ứng được chúng một cách hoàn toàn. Những nơi mà yêu cầu thiết kế bị phá vỡ gọi là các lỗ hổng.

2.2 Các lỗ hổng bảo mật của mạng máy tính :

2.2.1 Các điểm yếu của mạng máy tính :

Việc toàn cầu hoá các hoạt động thương mại làm cho sự phụ thuộc tương hỗ ngày càng tăng giữa các hệ thống thông tin. Việc chuẩn hoá công nghệ vì tính hiệu quả và kinh tế song cũng dẫn tới chuẩn hoá tính mỏng manh vốn có của mạng cho kẻ thù lợi dụng, Các quy tắc và tự do hoá cũng đóng góp cho việc tăng thêm tính nguy cơ của an toàn mạng. Có nhiều nguyên nhân gây ra lỗ hổng bao gồm:

1. Độ phức tạp: Các hệ thống phức tạp làm tăng xác suất của lỗ hổng, sai sót trong cấu hình hoặc truy cập ngoài ý muốn.

2. Tính phổ biến: Các loại mã, phần mềm, hệ điều hành và phần cứng có tính phổ biến sẽ làm tăng khả năng kẻ tấn công có thể tìm thấy hoặc có thông tin về các lỗ hổng đã biết.

3. Mức độ kết nối: Thiết bị càng được kết nối nhiều thì khả năng xuất hiện lỗ hổng càng cao.

4. Quản lý mật khẩu kém: Những mật khẩu yếu có thể bị phá bằng tấn công brute-force và việc sử dụng lại mật khẩu có thể dẫn đến từ một vi phạm dữ liệu trở thành nhiều vụ vi phạm xảy ra.

5. Lỗi hệ điều hành: Giống như bất kỳ phần mềm nào khác, hệ điều hành cũng có thể có lỗ hổng. Các hệ điều hành không an toàn – chạy mặc định và để tất cả mọi người dùng có quyền truy cập đầy đủ sẽ có thể cho phép vi-rút và phần mềm độc hại thực thi các lệnh.

6. Việc sử dụng Internet: Internet có rất nhiều loại phần mềm gián điệp và phần mềm quảng cáo có thể được cài đặt tự động trên máy tính.

7. Lỗi phần mềm: Lập trình viên có thể vô tình hoặc cố ý để lại một lỗi có thể khai thác trong phần mềm.

8. Đầu vào của người dùng không được kiểm tra: Nếu trang web hoặc phần mềm cho rằng tất cả đầu vào đều an toàn, chúng có thể thực thi các lệnh SQL ngoài ý muốn.

9. Con người: Lỗ hổng lớn nhất trong bất kỳ tổ chức nào là con người đằng sau hệ thống đó. Tấn công phi kỹ thuật (social engineering) là mối đe dọa lớn nhất đối với đa số các tổ chức.

Trên thực tế, người ta đã thống kê được các lỗ hỏng dễ bị xâm nhập thông qua mạng máy tính, cụ thể:

- Thiếu điều khiển truy cập bộ định tuyến và lập cấu hình sai ACL sẽ cho phép rò rỉ thông tin thông qua các giao thức ICMP, IP, NetBIOS, dẫn đến truy cập bất hợp pháp các dịch vụ trên máy phục vụ.

- Điểm truy cập từ xa không được theo dõi và bảo vệ sẽ là phương tiện truy cập dễ dàng nhất đối với mạng công ty.

- Rò rỉ thông tin có thể cung cấp thông tin phiên bản hệ điều hành và chương trình ứng dụng, người dùng, nhóm, địa chỉ tên miền cho kẻ tấn công thông qua chuyển vùng và các dịch vụ đang chạy như SNMP, finger, SMTP, telnet, rusers, sunrpc, NetBIOS.

- Máy chủ chạy các dịch vụ không cần thiết (như sunrpc, FTP, DNS, SMTP sẽ tạo ra lối vào thâm nhập mạng trái phép.

- Mật mã yếu, dễ đoán, dùng lại ở cấp trạm làm việc có thể dồn máy phục vụ vào chỗ thoả hiệp.

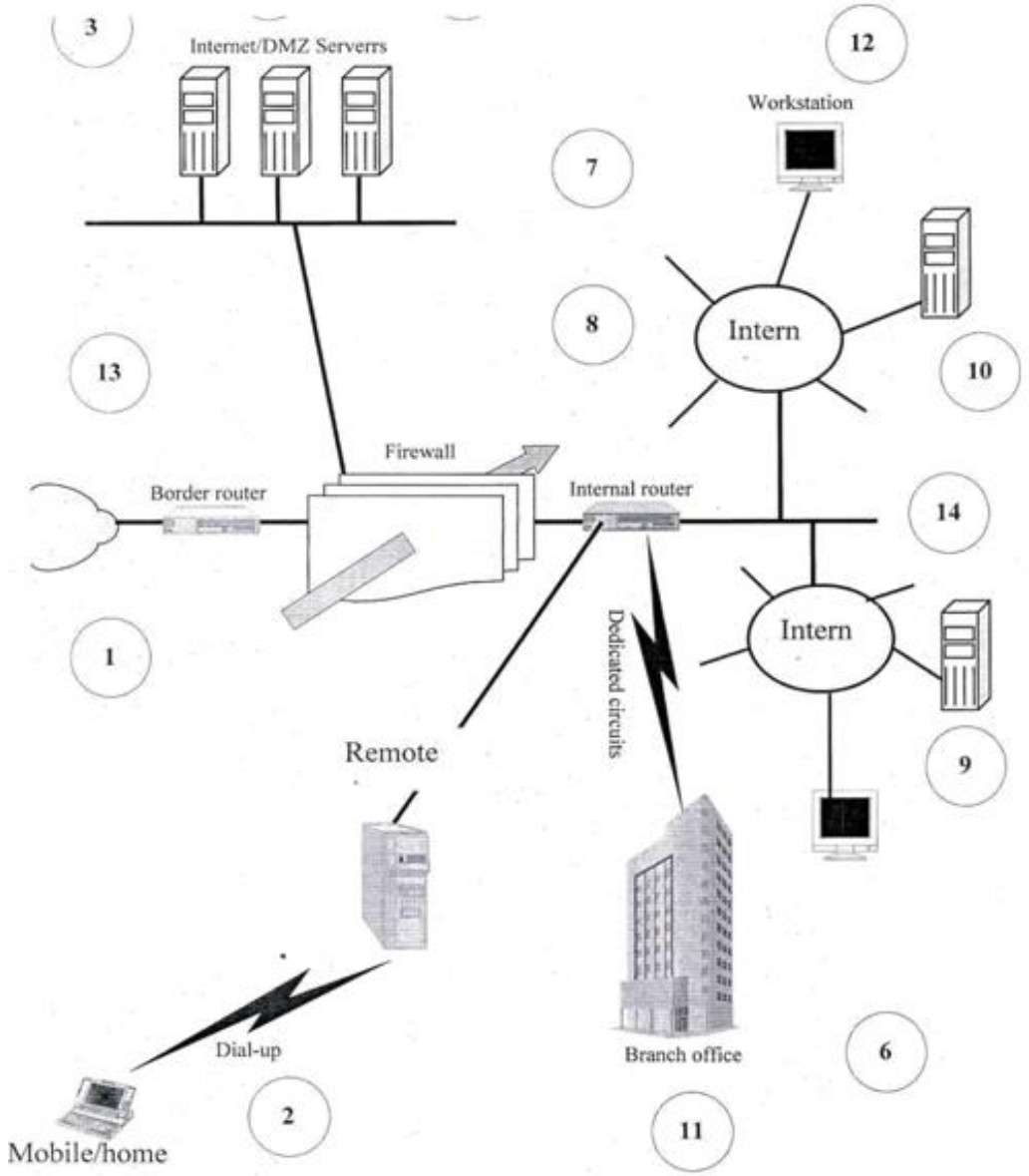
- Tài khoản người dùng hoặc tài khoản thử nghiệm có đặc quyền quá mức.

- Máy phục vụ Internet bị lập cấu hình sai, đặc biệt là kịch bản CGI trên máy phục vụ web và FTP nặc danh.

- Bức tường lửa hoặc ACL bị lập cấu hình sai có thể cho phép truy cập trực tiếp hệ thống trong hoặc một khi đã thoả hiệp xong máy phục vụ.

- Phần mềm chưa được sửa chữa, lỗi thời, dễ bị tấn công, hoặc để ở cấu hình mặc định.

- Quá nhiều điều khiển truy cập thư mục và tập tin.



Hình 2-1: Mô hình mạng máy tính

- Quá nhiều mối quan hệ uỷ quyền như NT domain Trusts, các tập tin.rhosts và hosts.equiv trong UNIX sẽ cho kẻ tấn công truy cập hệ thống bất hợp pháp.

- Các dịch vụ không chứng thực.

- Thiếu tính năng ghi nhật ký, theo dõi và dò tại mạng và cấp độ máy chủ.

- Thiếu chính sách bảo mật, thủ tục và các tiêu chuẩn tối thiểu.

2.2.2 Lỗ hổng theo khu vực phát sinh :

Bao gồm: Lỗ hổng code

- Lỗ hổng code xuất hiện do lỗi trong quá trình xây dựng phần mềm, gồm các lỗi logic, cú pháp và ở các mức truy cập. Lỗ hổng code còn bao gồm cả những cài đặt cố ý của nhà thiết kế để tiếp cận trái phép vào hệ thống của người dùng phần mềm.

- Lỗ hổng cấu hình.

- Lỗ hổng cấu hình, xuất hiện trong quá trình cài đặt, cấu hình và các phương tiện kỹ thuật của hệ thống thông tin , như các tham số cài đặt và thông số kỹ thuật của các thiết bị kỹ thuật.

- Lỗ hổng kiến trúc.

- Lỗ hổng kiến trúc, phát sinh trong quá trình thiết kế hệ thống thông tin .

- Lỗ hổng tổ chức tồn tại do thiếu (hoặc do các khiếm khuyết) của các biện pháp tổ chức bảo vệ thông tin trong các hệ thống thông tin , hoặc do không tuân thủ các quy tắc khai thác hệ thống bảo vệ thông tin của hệ thống thông tin.

2.2.3 Lỗ hổng phát sinh do các khiếm khuyết của hệ thống thông tin :

Trong hệ thống thông tin tồn tại những khiếm khuyết sẽ làm xuất hiện nhiều lỗ hổng. Ví dụ: những khiếm khuyết dẫn đến rò rỉ, hoặc lộ thông thông tin tiếp cận hạn chế; khiếm khuyết liên quan đến tràn bộ nhớ (khi phần mềm thực hiện các bản ghi dữ liệu vượt ra ngoài giới hạn của bộ nhớ vùng đệm, kết quả là dữ liệu được ghi phía trước hoặc tiếp sau bộ đệm bị hư hại).

Các khiếm khuyết của hệ thống thông tin làm phát sinh lỗ hổng an toàn thông tin thường liên quan đến các vấn đề như: cài đặt sai tham số trong đảm bảo chương trình, kiểm tra không đầy đủ dữ liệu đầu vào, khả năng giám sát đường tiếp cận các thư mục,

phân quyền sử dụng các lệnh của hệ điều hành (ví dụ, lệnh xem cấu trúc thư mục, lệnh sao chép, lệnh loại bỏ tệp từ xa); áp dụng các toán tử tích hợp ngôn ngữ lập trình, sử dụng mã lệnh, rò rỉ thông tin tiếp cận hạn chế, sử dụng các biến đổi mật mã, quản lý tài nguyên, tràn bộ nhớ.

2.2.4 Lỗ hổng theo vị trí phát hiện :

- Lỗ hổng trong đảm bảo chương trình toàn hệ thống: lỗ hổng hệ điều hành (lỗ hổng hệ thống tệp, lỗ hổng chế độ tải, lỗ hổng trong các cơ chế quản lý quy trình…), lỗ hổng hệ thống quản lý cơ sở dữ liệu.

- Lỗ hổng trong phần mềm ứng dụng.

- Lỗ hổng trong phần mềm chuyên dùng, tức là các lỗ hổng đảm bảo chương trình dùng để giải quyết các bài toán đặc thù của hệ thống thông tin, cụ thể là: lỗi lập trình, sự có mặt các chức năng không công bố có khả năng ảnh hưởng lên các phương tiện bảo vệ thông tin, khiếm khuyết trong các cơ chế hạn chế tiếp cận cho đến các đối tượng đảm bảo chương trình chuyên dùng.

- Lỗ hổng tồn tại trong đảm bảo chương trình của các phương tiện kỹ thuật như: phần sụn các thiết bị nhớ, các mạch logic tích hợp, các hệ thống đầu vào/ra, chương trình trong các bộ điều khiển, giao diện….

- Lỗ hổng trong các thiết bị cầm tay như: hệ điều hành các thiết bị di động, giao diện truy cập không dây....

- Lỗ hổng trong các thiết bị mạng như: bộ định tuyến, tổng đài, các trang bị viễn thông khác như: giao thức dịch vụ mạng, giao thức điều khiển thiết bị viễn thông....

- Lỗ hổng trong các thiết bị bảo vệ thông tin. Bao gồm lỗ hổng trong các phương tiện quản lý truy cập (kiểm soát tính toàn vẹn, phần mềm chống mã độc, hệ thống phát hiện xâm nhập, tường lửa…).

Bên cạnh đó, GOST P56546-2-15 còn phân loại lỗ hổng dựa trên các tiêu chí tìm kiếm như: tên của hệ điều hành, nền tảng phát triển, tên phần mềm và phiên bản, mức

độ nguy hại của lỗ hổng, ngôn ngữ lập trình và dịch vụ sử dụng để vận hành phần mềm.

2.2.5 Lỗ hổng đã biết, lỗ hổng zero-day :

Với những kẻ tấn công, lỗ hổng là những kênh chính để xâm nhập trái phép vào hệ thống thông tin . Do đó, tìm kiếm lỗ hổng luôn là mối quan tâm hàng đầu. Khi phát hiện được lỗ hổng, kẻ tấn công lập tức tận dụng cơ hội để khai thác. Từ thời điểm phát hiện ra lỗ hổng đến lần vá đầu tiên sẽ mất một khoảng thời gian dài và đây chính là cơ hội để thực hiện lây nhiễm, phát tán mã độc. Còn với các chuyên gia bảo mật thông tin, phát hiện và khắc phục lỗ hổng là nhiệm vụ quan trọng hàng đầu. Việc phát hiện lỗ hổng đã khó khăn, nhưng khắc phục còn khó khăn hơn. Do vậy, để thuận tiện trong quá trình khắc phục, các chuyên gia đã chia lỗ hổng thành hai loại là lỗ hổng đã biết và lỗ hổng zero-day.

Lỗ hổng đã biết, là lỗ hổng đã được công bố, kèm theo các biện pháp thích hợp để bảo vệ hệ thống thông tin , các bản vá lỗi và bản cập nhật. Như vậy, mỗi khi lỗ hổng được phát hiện thuộc loại này, thì vấn đề cũng coi như đã được giải quyết.

Tuy nhiên, có những lỗ hổng mà chỉ đến thời điểm phát hành bản cập nhật, hoặc phiên bản mới của sản phẩm, nhà sản xuất mới biết về sự tồn tại của nó. Nhà sản xuất không đủ thời gian để nghiên cứu và khắc phục sản phẩm đã phát hành, nên các lỗ hổng loại này được đặt tên là lỗ hổng zero-day. Như vậy, trong suốt thời gian kể từ thời điểm tồn tại đến khi bị phát hiện, lỗ hổng này có thể đã được khai thác trong thực tế và gây ảnh hưởng tới tổ chức, doanh nghiệp, người dùng.

Lỗ hổng zero-day thường tồn tại trong thời gian dài, trung bình khoảng 300 ngày. Một số có "tuổi thọ" cao hơn rất nhiều. Hãng SAP đã công bố rằng, họ từng phát hiện và vá được các lỗ hổng có tuổi thọ 10 năm. Trong đó, nguy hiểm nhất là các lỗ hổng: CVE-2004-308 (làm tổn hại bộ nhớ), CVE-2005- 2974 (gây tấn công từ chối dịch vụ) và CVE-2005-3550 (cho phép thực hiện lệnh từ xa).

Ngoài các hãng bảo mật, "hacker" cũng có thể là những người đầu tiên phát hiện ra lỗ hổng. Với các "hacker mũ trắng" thì các lỗ hổng zero-day là đối tượng nghiên cứu

hấp dẫn, nếu phát hiện và khắc phục được, họ cũng sẵn sàng thông báo cho nhà sản xuất. Nhưng với các "hacker mũ đen" thì đây là cơ hội tốt để trục lợi. Họ sẽ nghiên cứu phương án khai thác ngay lập tức, thậm chí đưa ra rao bán tại chợ đen với giá cao. Chẳng hạn, lỗ hổng zero-day cho phép chiếm quyền quản trị trên hệ điều hành Windows được rao bán với giá 90 nghìn USD. Tội phạm mạng hay các cơ quan đặc vụ sẵn sàng chi trả khoản tiền lớn để mua lại các lỗ hổng này, tạo nên thị trường chợ đen sôi động trên mạng Internet.

Vì thế, nhiều hãng bảo mật sẵn sàng chi những khoản tiền lớn để trả cho những ai phát hiện được lỗ hổng trong các sản phẩm của họ. Gần đây, Kaspersky Lab đã tăng tiền thưởng lên 100 nghìn USD cho người có thể phát hiện ra những lỗ hổng nghiêm trọng trong các sản phẩm của hãng này.

2.3 Một số phương thức tấn công mạng :

Tấn công mạng hay còn gọi là chiến tranh trên không gian mạng. Có thể hiểu tấn công mạng là hình thức tấn công xâm nhập vào một hệ thống mạng máy tính, cơ sở dữ liệu, hạ tầng mạng, website, thiết bị của một cá nhân hoặc một tổ chức nào đó.

Cụm từ "Tấn công mạng" có 2 nghĩa hiểu:

– Hiểu theo cách tích cực (positive way): Tấn công mạng (penetration testing) là phương pháp Hacker mũ trắng xâm nhập vào một hệ thống mạng, thiết bị, website để tìm ra những lỗ hổng, các nguy cơ tấn công nhằm bảo vệ cá nhân hoặc tổ chức.

– Hiểu theo cách tiêu cực (negative way): Tấn công mạng (network attack) là hình thức, kỹ thuật Hacker mũ đen tấn công vào một hệ thống để thay đổi đối tượng hoặc tống tiền.

Đối tượng bị tấn công có thể là cá nhân, doanh nghiệp, tổ chức hoặc nhà nước. Hacker sẽ tiếp cận thông qua mạng nội bộ gồm máy tính, thiết bị, con người). Trong yếu tố con người, hacker có thể tiếp cận thông qua thiết bị mobile, mạng xã hội, ứng dụng phần mềm.

Tóm lại, một cuộc tấn công không gian mạng có thể nhằm vào cá nhân, doanh

nghiệp, quốc gia, xâm nhập vào trong hệ thống, cơ sở hạ tầng mạng, thiết bị, con người dưới nhiều các khác nhau và mục tiêu khác nhau.

2.3.1 Tấn công vào trình duyệt (Browse Attacks)

Một trong các kiểu tấn công mạng điển hình nhất năm 2017 phải kể đến là tấn công vào trình duyệt. Các cuộc tấn công của trình duyệt thường được bắt đầu bằng những trang web hợp pháp nhưng dễ bị tổn thương. Kẻ tấn công có thể xâm nhập vào website và gây hại cho đối tượng bằng phần mềm độc hại.

Cụ thể, khi có khách truy cập mới thông qua trình duyệt web, trang web đó sẽ lập tức bị nhiễm mã độc. Từ đó, mã độc sẽ xâm nhập vào hệ thống của nạn nhân qua lỗ hổng của trình duyệt.Các trình duyệt web bị tin tặc tấn công chủ yếu năm 2017 là Microsoft Internet Explorer Edge, Google Chrome, Mozilla, Firefox, Apple Safari, Opera.

Hình 2-2: Tấn công vào trình duyệt Web

2.3.2 Tấn công bằng phần mềm độc hại Malware

Tấn công Malware: là một trong những hình thức tấn công qua mạng phổ biến nhất hiện nay. Malware bao gồm:

- Spyware (phần mềm gián điệp)
- Ransomware (mã độc tống tiền)
- Virus
- Worm (phần mềm độc hại lây lan với tốc độ nhanh)

Thông thường, Hacker sẽ tiến hành tấn công người dùng thông qua các lỗ hổng bảo mật. Hoặc lừa người dùng Click vào một đường Link hoặc Email (Phishing) để cài phần mềm độc hại tự động vào máy tính. Một khi được cài đặt thành công, Malware sẽ gây ra những hậu quả nghiêm trọng:

- Chặn các truy cập vào hệ thống mạng và dữ liệu quan trọng (Ransomware).
- Cài đặt thêm phần mềm độc hại khác vào máy tính người dùng.
- Đánh cắp dữ liệu (Spyware).
- Phá hoại phần cứng, phần mềm, làm hệ thống bị tê liệt, không thể hoạt động.

Hình 2-3: Tấn công bằng phần mềm độc hại

2.3.3 Tấn công giả mạo (Phishing)

Phishing (tấn công giả mạo) là hình thức tấn công mạng bằng giả mạo thành một đơn vị uy tín để chiếm lòng tin và yêu cầu người dùng cung cấp thông tin cá nhân cho chúng.

Thông thường, Hacker sẽ giả mạo là ngân hàng, ví điện tử, trang giao dịch trực tuyến hoặc các công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin cá nhân như: tài khoản & mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quan trọng khác.

Phương thức tấn công này thường được thực hiện thông qua việc gửi Email và tin nhắn. Người dùng khi mở Email và Click vào đường Link giả mạo sẽ được yêu cầu đăng nhập. Nếu "cắn câu", tin tặc sẽ có được thông tin cá nhân của người dùng ngay tức khắc.

Phương thức Phishing được phát hiện lần đầu tiên vào năm 1987. Thuật ngữ là sự kết hợp của 2 từ: Fishing For Information (câu thông tin) và Phreaking (trò lừa đảo sử

dụng điện thoại của người khác không trả phí). Do sự tương đồng trong việc "câu cá" và "câu thông tin người dùng", nên thuật ngữ Phishing ra đời.

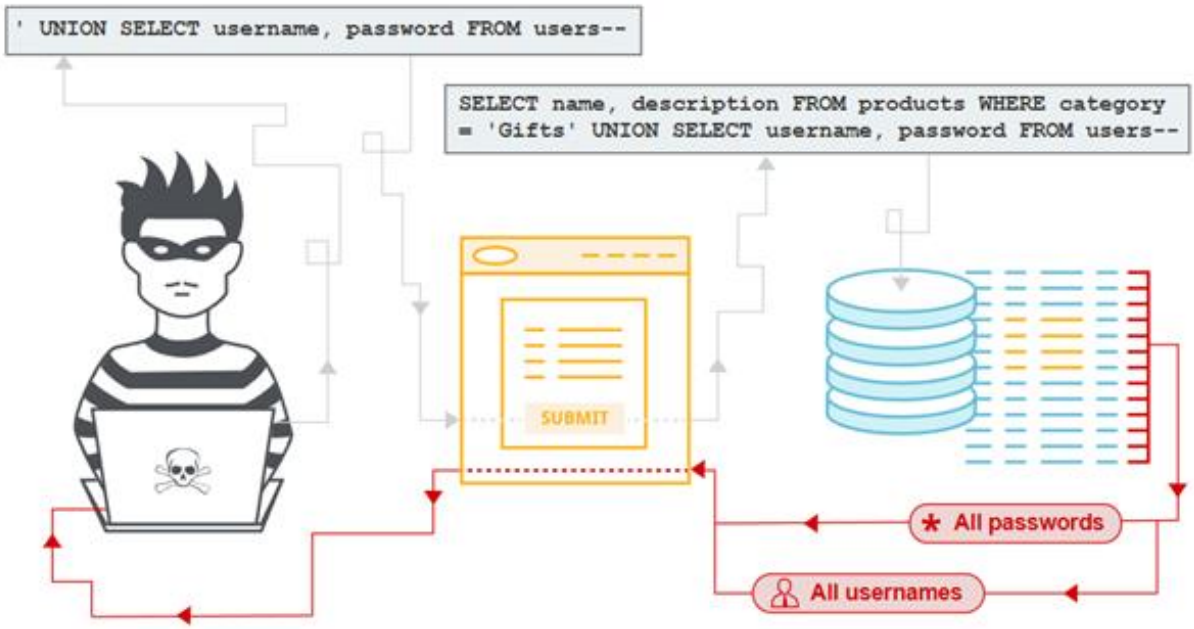
Hình 2-4: Tấn công từ chối dịch vụ (Ddos Attacks)

2.3.4 Tấn công cơ sở dữ liệu (SQL injection)

Các cuộc tấn công SQL Injection được thực hiện bằng cách gửi lệnh SQL độc hại đến các máy chủ cơ sở dữ liệu thông qua các yêu cầu của người dùng mà website cho phép. Bất kỳ kênh input nào cũng có thể được sử dụng để gửi các lệnh độc hại, bao gồm các thẻ <input> chuỗi truy vấn (query strings), cookie và tệp tin.

Với SQL injection các hacker có thể truy cập một phần hoặc toàn bộ dữ liệu trong hệ thống, có thể gây ra những thiệt hại khổng lồ

Với việc SQL injection dễ tấn công, phổ biến, gây ra hậu quả nghiêm trọng. Đó là lý do mà SQL injection đứng đầu trong 10 lỗ hổng bảo mật của OWASP.

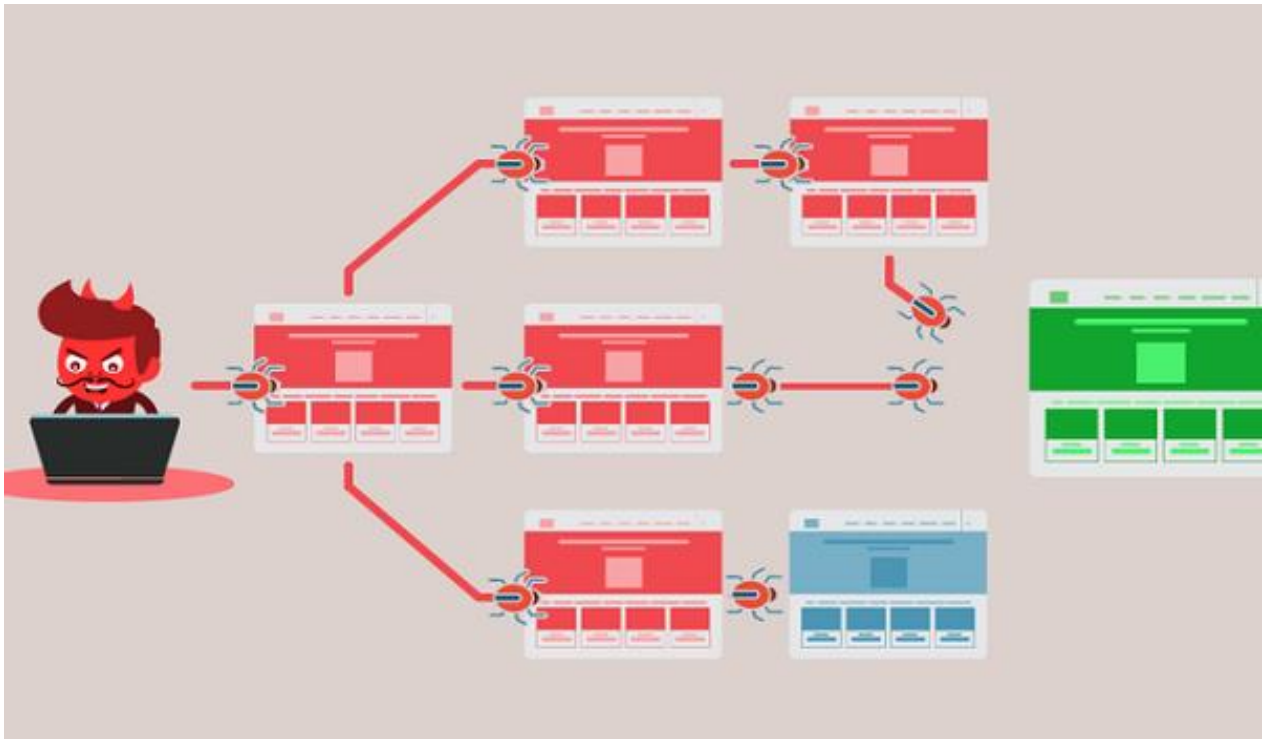


Hình 2-5: Tấn công cơ sở dữ liệu SQL injection

2.3.5 Tấn công từ chối dịch vụ (Ddos Attacks)

DoS (Denial of Service) là "đánh sập tạm thời" một hệ thống, máy chủ hoặc mạng nội bộ. Để thực hiện được điều này, các Hacker thường tạo ra một lượng Traffic/Request khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải. Theo đó, người dùng sẽ không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.

Một hình thức biến thể của DoS là DDoS (Distributed Denial of Service): Tin tặc sử dụng một mạng lưới các máy tính (Botnet) để tấn công người dùng.vấn đề ở đây là chính các máy tính thuộc mạng lưới Botnet sẽ không biết bản thân đang bị lợi dụng trở thành công cụ tấn công.



Hình 2-6: Tấn công từ chối dịch vụ (Ddos Attacks)

2.3.6 Kiểu tấn công rà quét

Thay vì sử dụng các hình thức tấn công toàn diện, Scan Attacks là kỹ thuật tấn công mạng rà quét lỗ hổng thông qua các dịch vụ, hệ thống máy tính, thiết bị, hạ tầng mạng của doanh nghiệp. Tin tặc sẽ sử dụng các công cụ để rà quét, nghe lén hệ thống mạng để tìm ra lỗ hổng sau đó thực thi tấn công.

2.3.7 Kiểu tấn công mạng khác

Ngoài 6 kiểu tấn công mạng nổi bật nói trên, Hacker còn có thể xâm nhập vào bên trong hệ thống bằng cách:

- Tấn công vật lý (Physical Attacks). Tin tặc sẽ cố gắng phá hủy, ăn cắp dữ liệu kiến trúc trong cùng một hệ thống mạng.

- Tấn công nội bộ (Insider Attacks). Các cuộc tấn công nội bộ thường liên quan tới người trong cuộc. Chẳng hạn như trong một công ty, một nhân viên nào đó “căm ghét” người khác… các cuộc tấn công hệ thống mạng nội bộ có thể gây hại hoặc vô hại. Khi có tấn công mạng nội bộ xảy ra, thông tin dữ liệu của công ty có thể bị truy cập trái

phép, thay đổi hoặc bán đổi.

CHƯƠNG 3: MỘT SỐ KỸ THUẬT PHỔ BIẾN PHÒNG VÀ PHÁT HIỆN XÂM NHẬP MẠNG MÁY TÍNH

3.1 Chữ kí số

3.1.1 Giới thiệu chung

Hàng ngày chúng ta vẫn thường hay dùng chữ ký để xác minh một vấn đề, hay để xác nhận quyền của mình đối với một vật thông qua những giấy tờ hoặc là một hợp đồng nào đó. Chẳng hạn như trên một bức thư nhận tiền từ ngân hàng, hay những hợp đồng ký kết mua bán, chuyển nhượng. Những chữ ký như vậy còn được gọi là chữ ký viết tay, bởi nó được viết bởi chính tay người ký không thể sao chụp được. Thông thường chữ ký viết tay trên các văn bản, trên các tài liệu hay trên các hợp đồng kinh tế..v.v.. thì được dùng để xác nhận người ký nó.

Sơ đồ chữ ký (hay còn gọi là chữ ký số) là phương pháp ký một bức điện lưu dưới dạng điện tử. Chẳng hạn một bức điện có chữ ký được truyền trên mạng máy tính. Chương này sẽ nghiên cứu vài sơ đồ chữ ký, song trước hết, ta sẽ thảo luận một vài khác biệt cơ bản giữa các chữ ký thông thường và chữ ký số.

Đầu tiên là vấn đề ký một tài liệu. Với chữ ký thông thường, nó là một phần vật lý của tài liệu, có nghĩa là chúng ta sử dụng chữ ký trên giấy làm cơ sở pháp lý cho sự xác thực người gửi. Việc phân tích chữ ký trên giấy phải đảm nhận được các tính chất sau:

- Người nhận có khả năng xác minh được chữ ký của người gửi.

- Không một ai (kể cả người nhận) có thể giả mạo được chữ ký của người gửi.

- Trong trường hợp người gửi phủ nhận chữ ký của mình trên một thông báo x nào đó, thì trọng tài phải có khả năng khẳng định được chữ ký trên x có phải là của người gửi hay không.

Tuy nhiên, một chữ ký số không gắn theo kiểu vật lý vào bức điện nên thuật toán

được dùng phải "không nhìn thấy" theo cách nào đó trên bức điện.

Thứ hai là vấn đề về kiểm tra. Chữ ký thông thường được kiểm tra bằng cách so sánh nó với các chữ ký xác thực khác. Ví dụ ai đó ký một tấm séc để mua hàng, người bán phải so sánh chữ ký trên mảnh giấy với chữ ký nằm ở mặt sau tấm thẻ tín dụng để kiểm tra. Đương nhiên đây không phải là phương pháp an toàn vì nó dễ dàng bị giả mạo. Mặt khác, các chữ ký số có thể được kiểm tra nhờ dùng một thuật toán kiểm tra công khai. Như vậy, bất kỳ ai cũng có thể kiểm tra được chữ ký số. Việc dùng một sơ đồ chữ ký an toàn có thể sẽ ngăn chặn được khả năng giả mạo.

Sự khác biệt cơ bản khác giữa chữ ký số và chữ ký thông thường là bản copy tài liệu được ký bằng chữ ký số đồng nhất với bản gốc, còn bản copy tài liệu có chữ ký trên giấy thường có thể khác với bản gốc. Điều này có nghĩa là phải cẩn thận ngăn chặn một bức điện ký số khỏi bị dùng lại. Ví dụ, nếu B ký một bức điện số xác nhận A rút 100$ từ tài khoản nhà băng của anh ta (ví dụ séc), anh ta chỉ muốn A có khả năng làm điều đó một lần. Vì thế, bản thân bức điện cần chứa thông tin (chẳng hạn như ngày tháng) để ngăn nó khỏi bị dùng lại.

Một sơ đồ chữ ký số thường chứa hai thành phần: thuật toán ký và thuật toán xác minh. B có thể ký bức điện x dùng thuật toán ký an toàn. Chữ ký sig(x) nhận được có thể được kiểm tra bằng thuật toán xác minh công khai ver(y). Khi cho trước cặp (x, y), thuật toán xác minh cho giá trị TRUE hay FALSE tuỳ thuộc vào việc chữ ký được xác thực như thế nào.

3.1.2 Chữ ký số (chữ ký điện tử)

Giống như chữ ký của người sử dụng trên các tài liệu thì chữ ký điện tử cũng có một ý nghĩa tương tự, đó là dùng chữ ký điện tử để ký lên một e- mail hoặc dữ liệu điện tử. Chữ ký điện tử được tạo ra và được chứng thực do việc dùng chứng chỉ số.

Ngày nay, trên thế giới đã có nhiều quốc gia đã ban hành những điều luật công nhận chữ ký điện tử có giá trị pháp lý như những chữ ký trên các văn bản, giấy tờ trước

đây vẫn dùng. Để ký, để tạo nên một giao dịch an toàn thì chứng chỉ số của người sử dụng là duy nhất.

Chữ ký điện tử mang lại cho người sử dụng nhiều chức năng quan trọng như:

♦ Tính xác thực

♦ An toàn và toàn vẹn dữ liệu

♦ Không chối cãi nguồn gốc

a. Tính xác thực.

Xác thực là sự chỉ ra đích danh một người (hoặc một host, một server, một client,…). Nó đảm bảo sự chính xác về người đã ký vào dữ liệu bởi vậy nên người sử dụng biết được ai đã tham gia vào một giao dịch và người tham gia vào giao dịch đó có phải là mạo danh hay không. Nó cũng cho phép một hệ thống kiểm soát được quyền truy cập của người dùng bằng việc thiết lập nên quyền truy cập hệ thống bằng chứng chỉ số.

b. Sự toàn vẹn dữ liệu.

Chữ ký điện tử bảo vệ sự toàn vẹn dữ liệu. Người sử dụng không thể biết được rằng một e- mail người sử dụng nhân được đã bị thay đổi hay chưa dù việc thay đổi đó là vô tình hay cố ý. Về mặt kỹ thuật thì chữ ký điện tử là việc mã hoá bởi khoá riêng của người gửi dữ liệu trên dạng băm của dữ liệu được gửi. Bất kỳ sự thay đổi nào sau khi tài liệu được ký đều không còn hợp lệ với dạng băm này.

Chữ ký điện tử đảm bảo sự tin tưởng vào dữ liệu- Chỉ người được chỉ định nhận mới đọc được thông tin đó.

c. Không chối cãi nguồn gốc.

Một đặc điểm của chữ ký điện tử là cho phép tác giả (người đã ký vào thông tin cần gửi đi) chứng minh quyền tác giả của mình. Không chối cãi nguồn gốc cho phép người sử dụng chứng minh được ai đã tham gia vào một giao dịch trước đó. Người đã ký tên vào một tài liệu điện tử thì không thể chối cãi được rằng mình đã không ký.

Vậy thì chối cãi nguồn gốc đơn giản là việc khi người nào đó đã ký vào một tài liệu điện tử thì không thể chối cãi là mình không ký.

3.1.3 Tạo và kiểm tra chữ ký điện tử.

Để tạo một chữ ký điện tử, người ký tạo một dữ liệu "băm" là duy nhất và rút ngắn lại so với dữ liệu gốc, sau đó dùng khoá riêng để mã hoá dữ liệu đã được "băm" nói trên. Vậy thì chữ ký điện tử chính là dạng băm của dữ liệu đã được mã hoá bằng khoá riêng của người ký. Nếu thông điệp bị thay đổi thì dẫn đến kết quả "băm" của thông điệp đã bị thay đổi khác so với kết quả "băm" của thông điệp khi chưa bị thay đổi.

Với các thông điệp khác nhau và với một khoá riêng dùng để ký thì chữ ký điện tử là duy nhất, bởi vậy không thể giả mạo được chữ ký điện tử. Chữ ký điện tử được thêm vào thông điệp và cả hai được gửi tới người nhận. Người nhận tạo lại giá trị băm từ thông điệp nhận được, sau đó dùng khoá công khai của người gửi để giải mã giá trị "băm" trong thông điệp nhận được. Nếu cả hai giá trị băm là giống nhau thì cả hai vấn đề chứng thực người gửi và tính toàn vẹn của thông tin.

3.1.4 Cơ sở lý luận của chữ ký số

Người ta sử dụng hệ mật mã để giải quyết một trong hai, hoặc cả hai loại bài toán: đó là bài toán bí mật và bài toán xác thực. Hệ mật mã giải quyết bài toán bí mật (gọi tắt là hệ mật) nhằm ngăn chặn các tổ chức và cá nhân bất hợp pháp thu nhận tin từ những bức điện gửi đi chỉ có người nhận hợp pháp mới đọc được. Còn hệ mật mã giải quyết bài toán xác thực (gọi tắt là hệ xác thực) thì nhằm ngăn chặn việc xen lấn trái phép những bức điện giả vào kênh công khai, bảo đảm cho người nhận, nhận được đúng nội dung điện của người gửi.

Theo tính chất khoá người ta phân các hệ mật mã ra làm hai loại, đó là hệ mật mã đối xứng hay còn gọi là hệ mật mã cổ điển (một khoá) và hệ mật mã phi đối xứng (hai khoá) hay còn gọi là hệ mật mã khoá công khai.

3.1.4.1 Hệ mật mã khoá công khai.

Hệ mật mã khoá công khai là hệ mật mã phi đối xứng, trong đó mỗi người sử dụng

công bố công khai một khoá cùng loại (tức là cùng lập mã hoặc cùng giải mã), nhưng giữ bí mật khoá kia của mình và khoá bí mật không thể tính toán để suy ra được từ khoá công khai (trong thời gian hợp lý).

Các khoá công khai của hệ có thể ghi vào một danh mục công khai. Do khoá bí mật không thể tính toán để suy ra được từ khoá công khai, nên biến đổi bí mật cũng không thể tính toán để suy ra được từ biến đổi công khai. Nếu ta gọi một biến đổi mà biến đổi ngược của nó không thể tính toán để suy ra được từ bản thân nó là biến đổi một chiều, thì mọi biến đổi công khai của hệ mật mã loại này sẽ đều là biến đổi một chiều. Việc không thể tính toán được ở đây là không thật chính xác theo quan điểm toán học. Nó phụ thuộc vào khả năng tính toán hiện tại của chúng ta, có nghĩa là phụ thuộc vào phương tiện kỹ thuật tính toán, vào các thuật toán đang được dùng. Vì vậy, một khoá bí mật có thể không thể tính toán được từ khoá công khai vào năm 2004, nhưng lại hoàn toàn có thể tính toán được từ nó vào năm 2200. Điều đó nhắc nhở những người thiết kế hệ mật mã khóa công khai cần phải trù tính tới sự phát triển của khoa học kĩ thuật trong một khoảng thời gian sắp đến để định ra các hệ số an toàn cho hệ.

3.1.4.2 Bí mật và xác thực bằng hệ mật mã khoá công khai

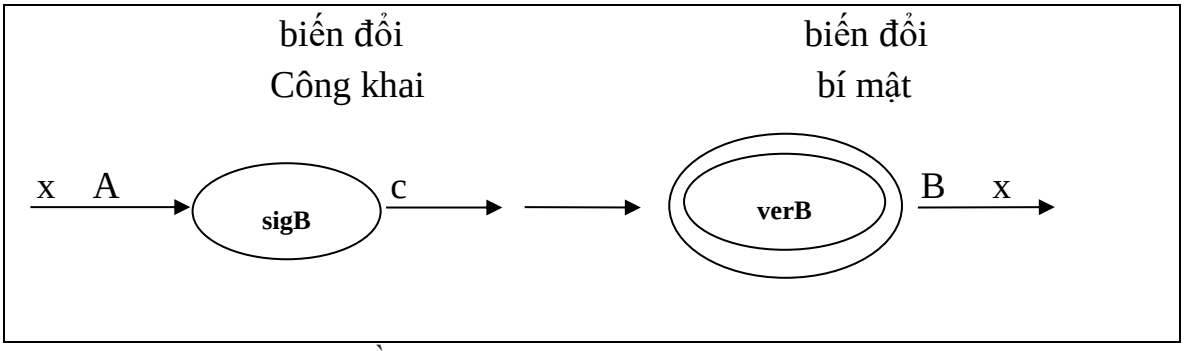
Hệ mật mã khoá công khai có thể được dùng như một hệ mật, hay một hệ xác thực hay vừa mật, vừa xác thực. Hệ mật mã khoá công khai là một hệ mật nếu như khoá công khai là khoá lập mã.

Giả sử trong hệ này người sử dụng A muốn gửi một thông báo x cho người sử dụng B. Khi đó vì A biết được khoá công khai eB của B (từ danh mục công khai), tức là biết được biến đổi lập mã sigB của B (như đã định nghĩa ở trên sig có nghĩa là thuật toán ký), nên anh ta có thể chuyển x cho B bằng cách gửi bản :

$$c = sigB(x).$$

Khi nhân được c, B có thể giải mã này bằng cách áp dụng vào c biến đổi bí mật verB của mình và thu được

verB(c) = verB(sigB(m)) =m.



Hình 3-1: Sơ đồ dùng hệ mật mã khoá công khai làm một hệ mật

Vì chỉ có B biết được khoá giải mã dB của mình, nên chỉ có anh ta mới biết được verB và giải được bản mã c thành bản rõ x. Như vậy thông báo m là hoàn toàn mật.

Sơ đồ trên không bảo đảm được tính xác thực của thông báo. Vì biến đổi sigB của B được công khai, nên bất kỳ người sử dụng nào cũng có thể thay thế thông báo x bằng một thông báo x' khác bằng cách gửi đi cho B bản mã c'=sigB(m') thay vào c.

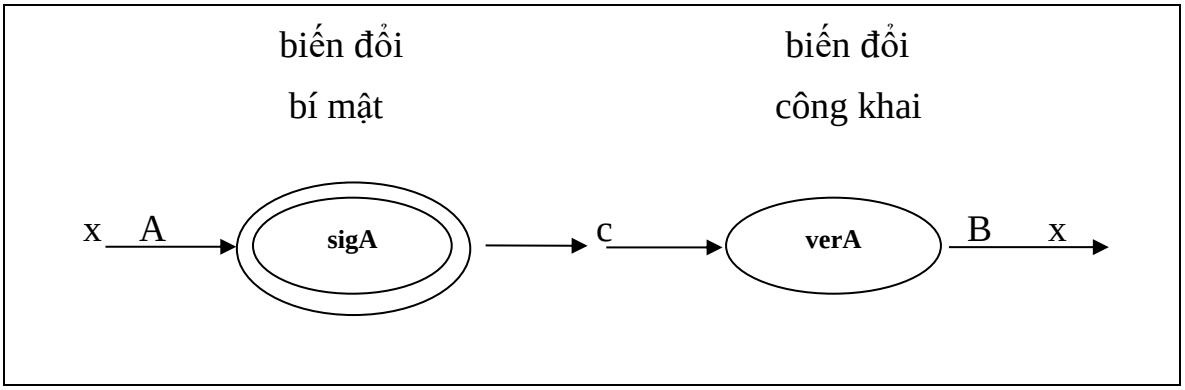
Hệ mật mã khoá công khai là một hệ xác thực nếu như khoá công khai là khoá giải mã.

Giả sử trong hệ này người sử dụng A muốn gửi một thông báo x cho người sử dụng B. Khi đó anh ta chuyển cho B bản mã

c = sigA(m).

Vì khoá giải mã dA, và do đó biến đổi giải mã verA, của A được công khai, nên khi nhận được c, người sử dụng B có thể áp dụng vào c biến đổi verA để giải bản mã c:

verA(c) = verA(sigA(x)) =m.



Hình 3-2: Sơ đồ dùng hệ mật mã khoá công khai làm một hệ xác thực

Vì chỉ có A biết được khoá eA, và do đó biết được biến đổi lập mã sigA của mình, nên chỉ có anh ta mới có khả năng tạo ra các bản mã bằng cách áp dụng sigA. Vì vậy thông báo x mà B nhân được đúng là do A gửi và nội dung đúng như A đã thảo ra. Điều đó có nghĩa là sơ đồ trên bảo đảm được tính xác thực của thông báo.

Sơ đồ này không bảo đảm được tính mật vì bất kỳ người sử dụng nào, do dA được công khai, cũng có thể giải được bản mã c và đọc được x.

Hệ mật mã khoá công khai là một hệ mật mã vừa mật vừa xác thực, nếu như nó thoả mãn hai điều kiện sau đây:

- Không gian bản rõ P phải trùng với không gian bản mã A, tức là P = A.

- Các biến đổi sigA và verA phải là các biến đổi nghịch đảo lẫn nhau, tức là: sigA(verA(x)) = x, verA(sigA(x)) = x thoả mãn cho mọi m $\in$P=A

Không làm mất tính chất chung, ta có thể giả thiết rằng trong hệ mật mã khoá công khai loại này, khoá công khai luôn là khoá lập mã.

Giả sử trong hệ mật mã khoá công khai vừa mật, vừa xác thực A muốn gửi một thông báo x cho B. Khi đó để đảm bảo cả tính mật và tính xác thực của x, A chuyển đi cho B bản mã

$$c = sigB(verA(x)).$$

Khi nhận được c, B giải bản mã này bằng cách áp dụng vào c trước hết biến đổi verB,và sau đó biến đổi sigA, tức là anh ta thực hiện

$$sigA(verB(c)) = sigA(verB(sigB(verA(x)))) = sigA(verA(x)) = x.$$

Thông báo m được đảm bảo tính mật vì chỉ có B biết được biến đổi verB, và do đó chỉ có anh ta đọc được bản mã c. Cả người gửi A và nội dung thông báo m được xác thực vì chỉ có A biết được verA, và do đó chỉ có anh ta mới có khả năng tạo ra các bản mã loại này.

3.1.4.3 Tổng quát hoá về sơ đồ chữ ký số bằng hệ mật mã khoá công khai

Mọi hệ mật mã khoá công khai xác thực đều có thể cung cấp cho ta một sơ đồ đơn

giản để tạo chữ ký số. Vì khoá lập mã eA được A giữ bí mật, nên biến đổi lập mã sigA cũng là biến đổi bí mật và chỉ có A biết. Do đó ta có thể coi sigA là chữ ký số của A.

Để gửi một thông báo x được A ký cho B, A tính

$$sA = sigA(x)$$

và gửi cặp (x, sA) cho B. Như vậy, sA được coi là chữ ký của A cho thông báo m. Khi nhận được (x, sA), B tính

$$verA(sA) = verA(sigA(x)).$$

Đẳng thức verA(sA) = x chứng tỏ rằng x là do chính A thảo ra. Như vậy là cả người gửi và nội dung thông báo m được xác thực. Vì chỉ có A biết được sigA, nên bất kỳ ai, kể cả B, đều không thể giả mạo được chữ ký của A trên một thông báo bất kỳ khác. Bản thân A cũng không thể phủ nhận được một thông báo đã ký của mình (với giả thiết là sigA không bị mất và không bị tổn thương). Mặt khác, vì verA được công khai, nên người nhận B có khả năng kiểm tra được chữ ký của A. Trong trường hợp giữa A và B xảy ra sự bất đồng, B trình trọng tài cặp (x, sA). Để giải quyết sự bất đồng trên, trọng tài tính verA(sA) và kiểm tra xem verA(sA) có đúng là x hay không. Như vậy, có thể coi sA =sigA(x) như là chữ ký số của A trên thông báo x

Sơ đồ chữ ký số trong hệ mật mã khoá công khai xác thực:

1. Trong hệ mật mã khoá công khai xác thực (với khoá bí mật là khoá lập mã, sA =sigA(x) là chữ ký số của A cho thông báo x. Chữ ký sA có các tính chất tương tự như chữ ký trên giấy. Cặp (x, sA) lầ thông báo đã được A ký và gửi đi cho B.

2. Sau khi nhận được (x, sA), B tính verA(sA). Đẳng thức verA(sA) = x chứng tỏ x do A thảo ra và gửi đi cho B. Nếu bất đẳng thức verA(sA) ≠ x chứng tỏ x đã bị giả mạo.

3. Trong trường hợp tranh chấp với A, B trình trọng tài cặp (x, sA). Trọng tài giải quyết sự tranh chấp này bằng cách tính verA(sA) và kiểm tra xem verA(sA) có đúng

bằng x hay không như B làm trong phần trên không.

Trong hệ mật mã khoá công khai vừa mật vừa xác thực với khoá công khai là khoá lập mã, ngoài việc đảm bảo tính xác thực ta còn phải đảm bảo cả tính mật của các thông báo gửi đi nữa. Do vậy, thủ tục tạo và kiểm tra chữ ký số cũng như thủ tục giải quyết tranh chấp có phức tạp hơn so với việc giải quyết các vấn đề trên trong hệ mật mã khoá công khai xác thực. Các thủ tục đó ta tóm tắt lại trong các điểm sau:

Chữ ký số trong hệ mật mã khoá công khai vừa mật, vừa xác thực:

1. Trong hệ mật mã khoá công khai vừa mật, vừa xác thực với khoá công khai là khoá lập mã, chữ ký số sA của A cho thông báo x được tính bằng cách áp dụng verA vào x tức là sA = verA(x).
2. Sau đó để giữ bí mật thông báo x, A sử dụng sigB để mã hoá A. Anh ta thu được c = sigB(sA) và gửi c cho B.
3. B trước hết sử dụng verB để giải mã c:

$$verB(c) = verB(sigB(sA)) = sA$$

và thu được chữ ký số sA của A cho thông báo x. Sau đó B áp dụng sigA vào sA để khôi phục bản rõ x.

$$sigA(sA) = sigA(verA(x)) = x.$$

Bây giờ B đã có cặp (x, sA) là thông báo có chữ ký của A với các tính chất tương tự như thông báo được ký trên giấy.

4. Khi xảy ra tranh chấp với A, B trình trọng tài cặp (x, sA). Trọng tài giải quyết sự tranh chấp này bằng cách tính sigA(sA) và kiểm tra xem sigA(sA) có đúng là x không.

Các hệ mật mã kinh điển tuy bảo đảm được sự xác thực nội dung thông báo, nhưng không thể dùng để giải quyết bất đồng giữa người gửi và người nhận được. Do người gửi và người nhận có cùng chung một khóa, người nhận có thể giả mạo chữ ký của người gửi, và vì thế trọng tài không thể giải quyết được sự bất đồng nảy sinh giữa hai người đó.

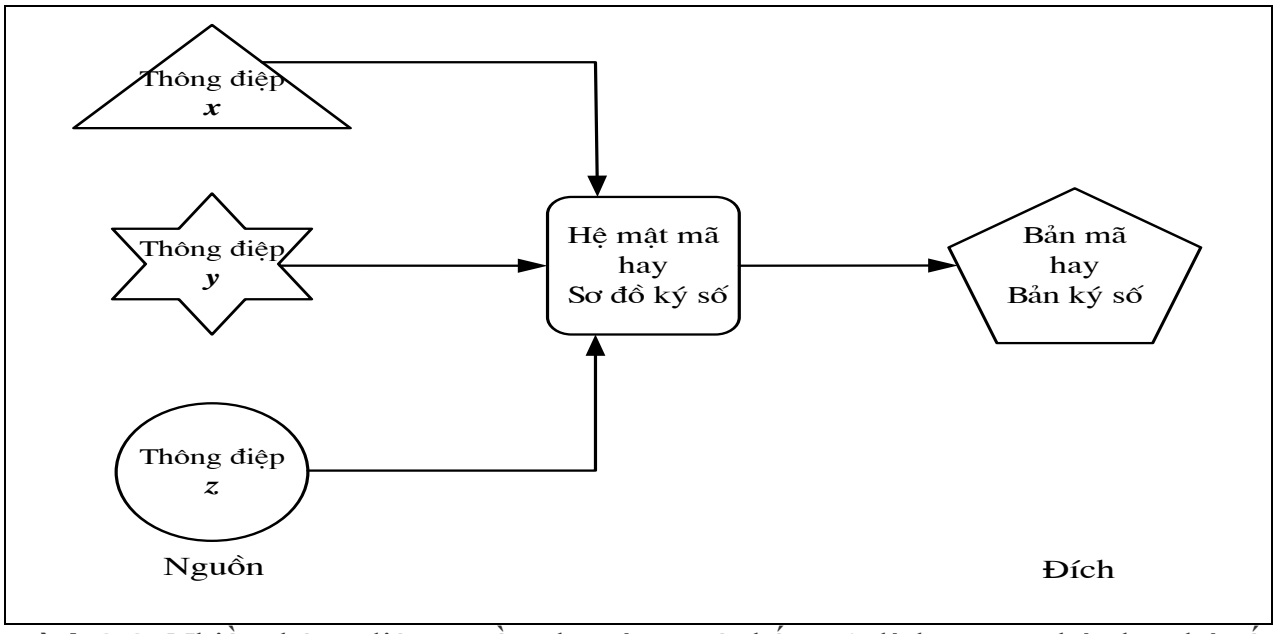
3.2 Hàm băm – Hash

3.2.1 Vai trò, vị trí của hàm Hash trong bảo vệ thông tin

Ngày nay, việc tổ hợp các mạng thông tin với máy tính đã trở nên phổ biến và đã mang lại lợi ích to lớn cho con người trong kinh tế, xã hội, an ninh quốc phòng... Nhưng thực tế hơn, chúng ta thấy rằng khi các hoạt động trong mọi lĩnh vực dựa trên các ứng dụng của Công nghệ thông tin thực sự bùng nổ thì phạm vi hoạt động cho các hoạt động gian lận, xâm phạm bất hợp pháp ngày càng trở nên vô cùng rộng lớn. Với sự phổ biến rộng rãi của kiến thức tin học, các hành vi gian lận qua máy tính có xu hướng ngày càng gia tăng và gia tăng rất mạnh, nhất là khi điểm yếu của hệ thống cũ được biết rõ. Chúng ta có thể đi đến kết luận rằng, các biện pháp an toàn cổ điển thông qua việc kiểm soát xâm nhập ở mức vật lý còn không đủ để đáp ứng nhu cầu trong công nghệ cao. Các biện pháp bảo đảm an toàn dữ liệu đáng tin cậy là những biện pháp dựa trên mật mã học và được thi hành một cách đúng đắn. Nghiên cứu để đưa ra các giải pháp mã hoá cao cấp cho nhu cầu an toàn dữ liệu đang là một chủ đề lớn của việc thiết kế và quản lý hệ thống thông tin.

3.2.2 Khái niệm thông điệp đại diện, hàm băm

Việc sử dụng các hệ mật mã và các sơ đồ chữ ký số thường là mã hóa và ký số trên từng bit của thông tin, thời gian để mã hóa và ký sẽ tỷ lệ thuận với dung lượng của thông tin. Thêm vào đó có thể xảy ra trường hợp: Với nhiều bức thông điệp đầu vào khác nhau, sử dụng hệ mật mã, sơ đồ ký số giống nhau (có thể khác nhau) thì cho ra kết quả bản mã, bản ký số giống nhau (ánh xạ N-1: nhiều – một). Điều này sẽ dẫn đến một số rắc rối về sau cho việc xác thực thông tin.



Hình 3-3: Nhiều thông điệp nguồn cho cùng một kết quả đích sau mã hóa hay ký số.

Với các sơ đồ ký số, chỉ cho phép ký các bức thông điệp (thông tin) có kích thước nhỏ và sau khi ký, bản ký số có kích thước gấp đôi bản thông điệp gốc – ví dụ với sơ đồ chữ ký chuẩn DSS chỉ ký trên các bức thông điệp có kích thước 160 bit, bản ký số sẽ có kích thước 320 bit. Trong khi đó trên thực tế, ta cần phải ký các thông điệp có kích thước lớn hơn nhiều, chẳng hạn vài chục MegaByte. Hơn nữa, dữ liệu truyền qua mạng không chỉ là bản thông điệp gốc, mà còn bao gồm cả bản ký số (có dung lượng gấp đôi dung lượng bản thông điệp gốc), để đáp ứng việc xác thực sau khi thông tin đến người nhận.

Một cách đơn giản để giải bài toán (với thông điệp có kích thước vài chục MB) này là chặt thông điệp thành nhiều đoạn 160 bit, sau đó ký lên các đoạn đó độc lập nhau. Nhưng, biện pháp này có một số vấn đề trong việc tạo ra các chữ ký số:

Thứ nhất: với một thông điệp có kích thước a, thì sau khi ký kích thước của chữ ký sẽ là 2a (trong trường hợp sử dụng DSS).

Thứ hai: với các chữ ký "an toàn" thì tốc độ chậm vì chúng dùng nhiều phép tính số học phức tạp như số mũ modulo.

Thứ ba: vấn đề nghiêm trọng hơn đó là kết quả sau khi ký, nội dung của thông điệp

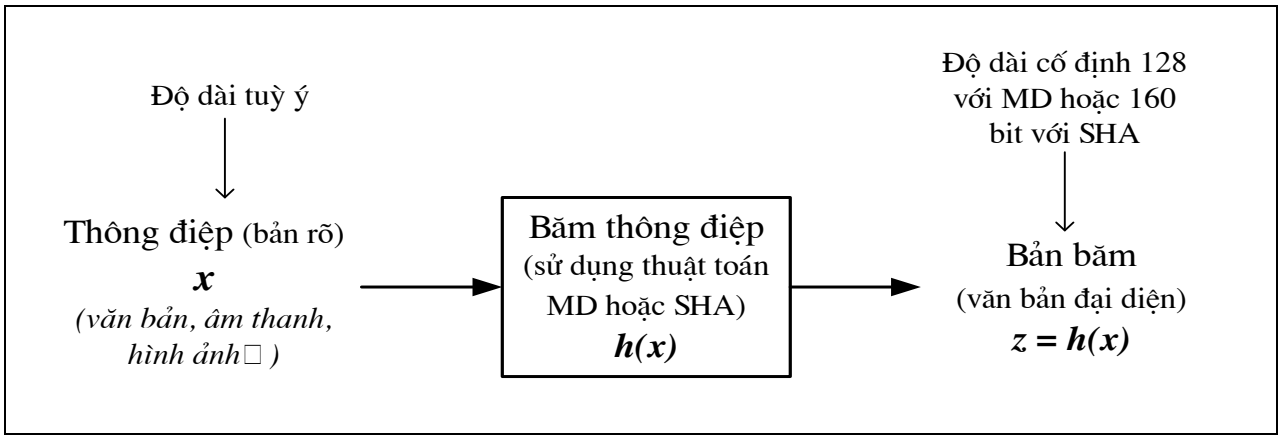
có thể bị xáo trộn các đoạn với nhau, hoặc một số đoạn trong chúng có thể bị mất mát, trong khi người nhận cần phải xác minh lại thông điệp. Ta cần phải bảo vệ tính toàn vẹn của thông điệp.

Giải pháp cho các vấn đề vướng mắc đến chữ ký số là dùng thông điệp đại diện và hàm băm để trợ giúp cho việc ký số. Các thuật toán băm với đầu vào là các bức thông điệp có dung lượng, kích thước tùy ý (vài KB đến vài chục MB thậm chí hơn nữa) – các bức thông điệp có thể là dạng văn bản, hình ảnh, âm thanh, file ứng dụng v.v… - và với các thuật toán băm: MD2, MD4, MD5, SHA cho các bản băm đầu ra có kích thước cố định: 128 bit với dòng MD, 160 bit với SHA.

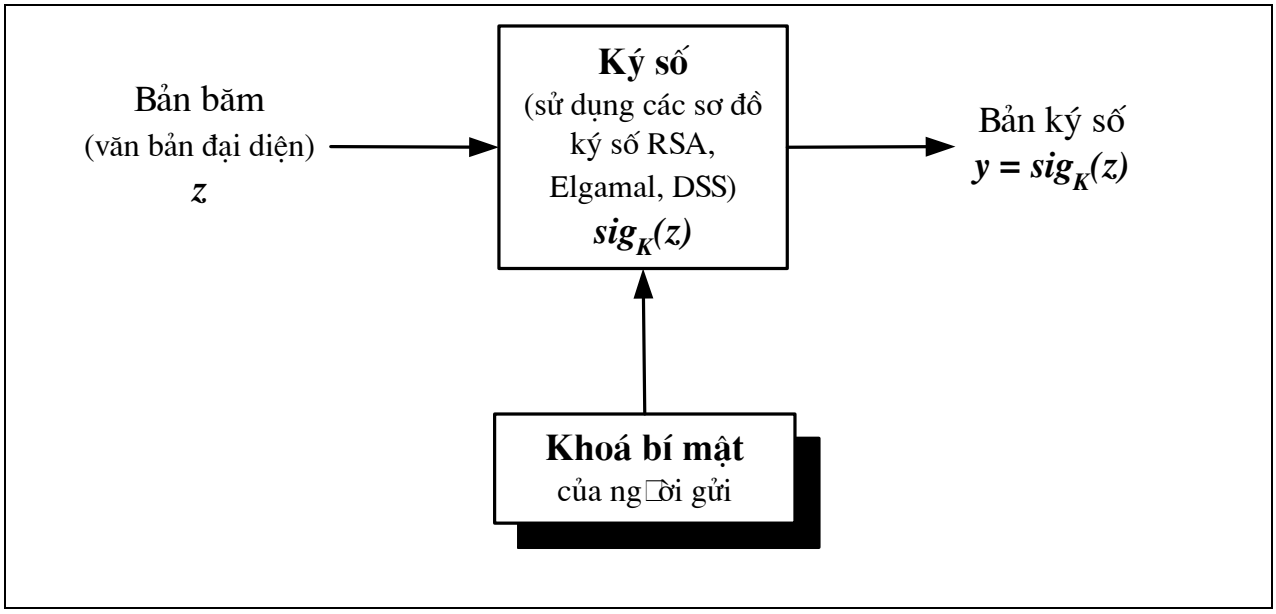
Khái niệm thông điệp đại diện : Bức thông điệp kích thước tùy ý sau khi băm sẽ được thu gọn thành những bản băm – được gọi là các thông điệp đại diện hay văn bản đại diện – có kích thước cố định (128 bit hoặc 160 bit).

Với mỗi thông điệp đầu vào chỉ có thể tính ra được một văn bản đại diện – giá trị băm tương ứng– duy nhất. Giá trị băm được coi là đặc thù của thông điệp, giống như dấu vân tay của mỗi người. Hai thông điệp khác nhau chắc chắn có hai văn bản đại diện khác nhau. Khi đã có văn bản đại diện duy nhất cho bức thông điệp, áp dụng các sơ đồ chữ ký số ký trên văn bản đại diện đó.

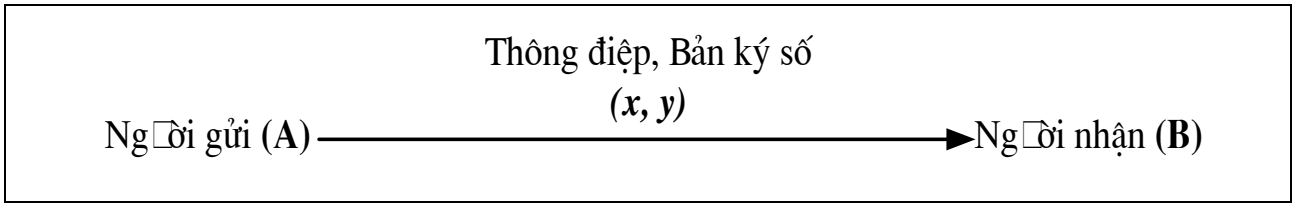
Cơ chế gửi thông tin sử dụng hàm băm trợ giúp cho chữ ký số được mô tả theo thứ tự các Hình 3-4a, 3-4b, 3-4c.



Hình 3-4a: Băm thông điệp.



Hình 3-4b: Ký trên bản băm.



Hình 3-4c: Truyền dữ liệu thông tin cần gửi.

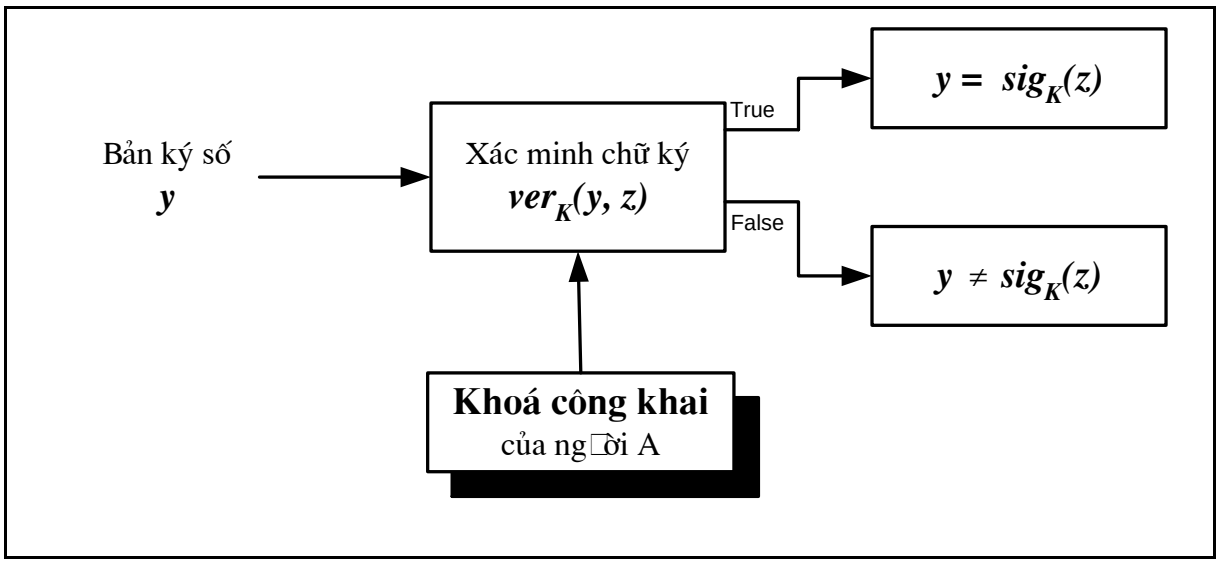
Hình 3-4: Sơ đồ mô tả các công đoạn người gửi A làm trước khi gửi thông điệp cho người B (sử dụng hàm băm rồi ký số).

Giả sử A muốn gửi cho B thông điệp x. A thực hiện các bước sau:

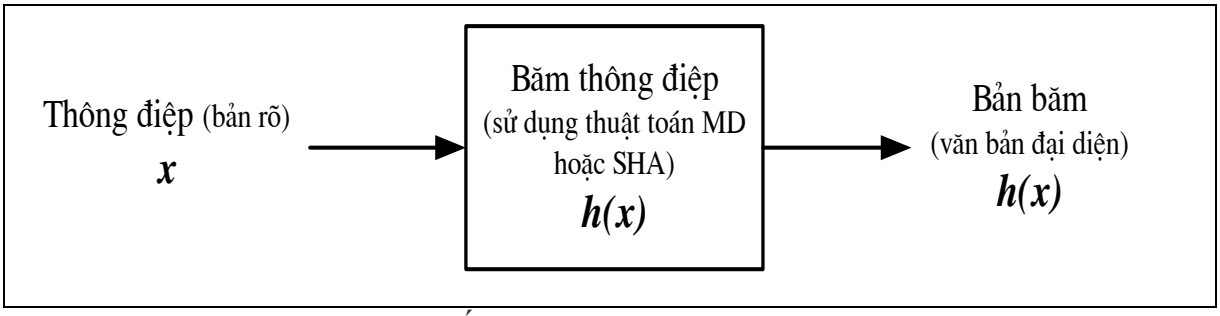
1. A băm thông điệp x (Hình 3-4a), thu được bản đại diện z = h(x) – có kích thước cố định 128 bit hoặc 160 bit.
2. A ký số trên bản đại diện z (Hình 3-4b), bằng khóa bí mật của mình, thu được bản ký số $y = sig_{K_1}(z)$.
3. A gửi (x, y) cho B (Hình 3-4c).

Khi B nhận được (x, y). B thực hiện các bước sau:

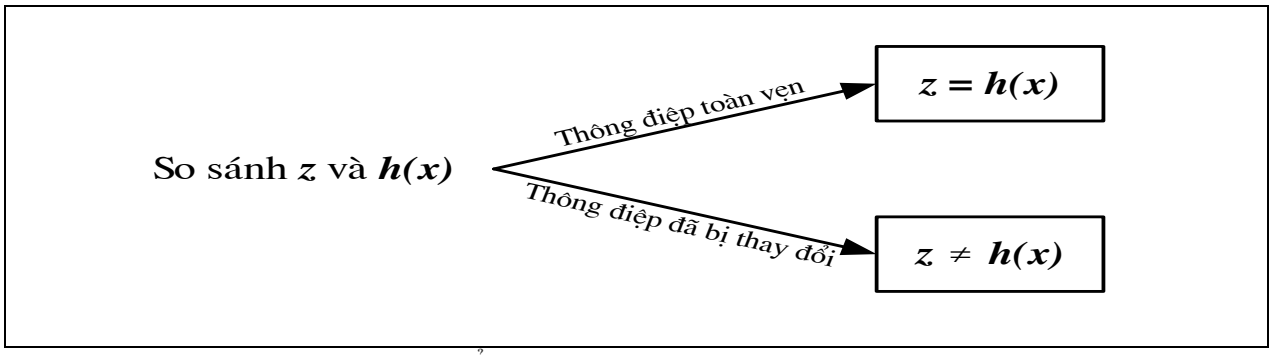
1. B kiểm tra chữ ký số để xác minh xem thông điệp mà mình nhận được có phải được gửi từ A hay ko bằng cách giải mã chữ ký số y, bằng khóa công khai của A, được z. (Hình 3-5a)
2. B dùng một thuật toán băm – tương ứng với thuật toán băm mà A dùng – để băm thông điệp x đi kèm, nhận được h(x). (Hình 3-5b)
3. B so sánh 2 giá trị băm z và h(x), nếu giống nhau thì chắc chắn rằng thông điệp x – mà A muốn gửi cho B – còn nguyên vẹn, bên cạnh đó cũng xác thực được người gửi thông tin là ai. (Hình 3-5c)



Hình 3-5a: Xác minh chữ ký.



Hình 3-5b: Tiến hành băm thông điệp x đi kèm.



Hình 3-5c: Kiểm tra tính toàn vẹn của thông điệp.

Hình 3-5: Sơ đồ mô tả các công đoạn sau khi người B nhận được thông điệp.

Hàm băm đã trợ giúp cho các sơ đồ ký số nhằm giảm dung lượng của dữ liệu cần thiết để truyền qua mạng (lúc này chỉ còn bao gồm dung lượng của bức thông điệp gốc và 256 bit (sử dụng MD) hay 320 bit (sử dụng SHA) của bức ký số được ký trên bản đại diện của thông điệp gốc), tương đương với việc giảm thời gian truyền tin qua mạng.

Hàm băm thường kết hợp với chữ ký số để tạo ra một loại chữ ký điện tử vừa an toàn hơn (không thể cắt/dán) vừa có thể dùng để kiểm tra tính toàn vẹn của thông điệp.

Hàm băm được ứng dụng rất mạnh trong vấn đề an toàn thông tin trên đường truyền. Các ứng dụng có sử dụng hàm băm không chỉ đảm bảo về mặt an toàn thông tin, mà còn tạo được lòng tin của người dùng vì họ có thể dễ dàng phát hiện được thông tin của mình có còn toàn vẹn hay không, họ biết rằng thông tin của mình chắc chắn được bí mật với phía các nhà cung cấp.

3.2.3 Định nghĩa hàm băm

Hàm băm (hash function) là một ánh xạ H từ một tập hợp X có số chiều n tùy ý

vào một tập hợp Y có số chiều k cố định (k < n) và thỏa mãn các điều kiện sau đây:

1. H là hàm một chiều, nghĩa là cho trước một phần tử x ϵ X thì việc tính H(x) = y ϵ Y là dễ dàng nhưng nếu cho trước y ϵ Y hãy tìm phần tử x ϵ X sao cho H(x) = y là một bài toán khó.

2. H là hàm va chạm yếu (weak Collision), nghĩa là cho trước một phần tử x ϵ X và y = H(x) thì việc tìm một phần tử x1 sao cho H(x1) = y là bài toán khó. Và

3. H là một hàm có va chạm mạnh, tức là việc tìm được 2 phần tử x, x1 với x ≠ x1 sao cho H(x) = H(x1) là không thể trong thực hành.

3.2.4 Đặc tính của hàm băm

Hàm băm h là hàm băm một chiều (one-way hash) với các đặc tính sau:

- Với thông điệp đầu vào x thu được bản băm z = h(x) là duy nhất.

- Nếu dữ liệu trong thông điệp x thay đổi hay bị xóa để thành thông điệp x' thì h(x') ≠ h(x). Cho dù chỉ là một sự thay đổi nhỏ hay chỉ là xóa đi 1 bit dữ liệu của thông điệp thì giá trị băm cũng vẫn thay đổi. Điều này có nghĩa là: hai thông điệp hoàn toàn khác nhau thì giá trị hàm băm cũng khác nhau.

- Nội dung của thông điệp gốc không thể bị suy ra từ giá trị hàm băm. Nghĩa là: với thông điệp x thì dễ dàng tính được z = h(x), nhưng lại không thể (thực chất là khó) suy ngược lại được x nếu chỉ biết giá trị hàm băm h(x).

3.3 Một số tuật toán băm

3.3.1 RIPEMD-128

RIPEMD-128 là một hàm băm 128 bit sử dụng xây dựng như mở rộng của Thuật toán Merkle Damgard : hàm băm được xây dựng bằng cách duyệt một chức năng nén 128 bit mà mất như một đầu vào 512 bit với đầu ra là 128 bit.

Các chức năng nén RIPEMD-128 dựa trên MD4, với các đặc thù mà nó sử dụng hai trường hợp song song của nó, Chúng ta phân biệt hai chi nhánh tính toán của nhánh

trái và nhánh phải và chúng ta hiển thị bởi Xi (resp.Yi) 32 bit của nhánh trái (resp.right branch).Quá trình này sẽ được cập nhật trong bước i của hàm nén .Quá trình này bao gồm 64 bước chia thành 4 vòng 16 bước từng ở cả hai chi nhánh cụ thể về quá trình:

Khởi tạo: Các đầu vào 128-bit chuỗi cvi biến được chia thành 4 từ hi mỗi 32 bit, sẽ sử dụng để khởi tạo các nhánh trái và phải 128 bit trạng thái nội bộ :

$$X_{-3} = h_0 \quad X_{-2} = h_1 \quad X_{-1} = h_2 \quad X_0 = h_3$$
$$Y_{-3} = h_0 \quad Y_{-2} = h_1 \quad Y_{-1} = h_2 \quad Y_0 = h_3 \ .$$

Mở rộng tin: Khối tin đầu vào 512 -bit được chia thành 16 từ Mi của mỗi 32 bit . mỗi từ Mi sẽ được sử dụng một lần trong mỗi vòng theo một thứ tự hoán vị (tương tự như MD4) và cho cả 2 nhánh.

$$W^l_{j\cdot 16+k} = M_{\pi^l_j(k)} \quad \text{and} \quad W^r_{j\cdot 16+k} = M_{\pi^r_j(k)}$$

Chức năng của từng bước: Tại mỗi bước i ,sổ đăng ký Xi+1 và Yi+1 được cập nhật với các chức năng f^1_j và f^r_j điều đó phụ thuộc vào những vòng j trong mà i thuộc về:

$$X_{i+1} = (X_{i-3} \boxplus \Phi^l_j(X_i, X_{i-1}, X_{i-2}) \boxplus W^l_i \boxplus K^l_j)^{\lll s^l_i},$$
$$Y_{i+1} = (Y_{i-3} \boxplus \Phi^r_j(Y_i, Y_{i-1}, Y_{i-2}) \boxplus W^r_i \boxplus K^r_j)^{\lll s^r_i},$$

Kết thúc quá trình: Một quyết toán và một feed-forward được áp dụng khi tất cả 64 bước đã được tính toán trong cả 2 chi nhánh . Bốn 32 -bit từ hi' soạn ra chuỗi biến cuối cùng đã thu được bằng cách :

$$h'_0 = X_{63} \boxplus Y_{62} \boxplus h_1 \quad h'_1 = X_{62} \boxplus Y_{61} \boxplus h_2$$
$$h'_2 = X_{61} \boxplus Y_{64} \boxplus h_3 \quad h'_3 = X_{64} \boxplus Y_{63} \boxplus h_0 \ .$$

3.3.2 RIPEMD-160

RIPEMD-160 là một hàm băm mật mã 160-bit, được thiết kế bởi Hans Dobbertin,

Antoon Bosselaers và Bart Preneel. Nó được thiết kế để sử dụng như là một thay thế an toàn cho các hàm băm 128-bit MD4, MD5 và RIPEMD. MD4 và MD5 được phát triển bởi Ron Rivest cho RSA Data Security, trong khi RIPEMD được phát triển trong khuôn khổ của dự án RIPE EU (RACE Integrity Primitives Evaluation, 1988-1992). Có hai lý chính để xem đây là một sự thay đổi tốt :

- Một kết quả băm 128-bit không cung cấp đủ bảo vệ nữa, một cuộc tấn công brute force vào hàm 128 bit chỉ đòi hỏi 264 hoặc 2.1019 giá trị của hàm. Năm 1994 Paul van Oorschot và Mike Wiener cho thấy việc brute- lực lượng này có thể được thực hiện trong vòng chưa đầy một tháng với một khoản đầu tư $10.000.000

- Trong nửa đầu năm 1995 Hans Dobbertin tìm thấy va chạm đối với một phiên bản của RIPEMD hạn chế đến hai vòng cùng của ba .Sử dụng kỹ thuật tương tự được sản xuất Hans vào mùa thu năm 1995 cho các va chạm (tất cả 3 vòng) MD4 . Cuộc tấn công vào MD4 chỉ đòi hỏi một vài giây trên một máy tính , và vẫn còn để lại một ít tự do để lựa chọn các tin nhắn, cầm quyền rõ ràng ra MD4 như là một hàm băm kháng va chạm . Ngay sau đó , vào mùa xuân năm 1996, Hans cũng tìm thấy va chạm cho các chức năng nén MD5. Mặc dù chưa được mở rộng đến va chạm với MD5 bản thân, cuộc tấn công này phôi nghi ngờ nghiêm trọng về sức mạnh của MD5 là một vụ va chạm

RIPEMD - 160 là một phiên bản được tăng cường của RIPEMD với một kết quả băm 160 -bit, và dự kiến sẽ được an toàn trong mười năm tới hoặc hơn. Triết lý thiết kế là xây dựng càng nhiều càng tốt về kinh nghiệm thu được bằng cách đánh giá MD4 , MD5 , và RIPEMD. Giống như người tiền nhiệm của nó, RIPEMD - 160 được điều chỉnh cho bộ vi xử lý 32 -bit , mà chúng ta cảm thấy sẽ vẫn quan trọng trong thập kỷ tới .

RIPEMD-256 và RIPEMD-320 là phần mở rộng tùy chọn tương ứng cho RIPEMD - 128 và RIPEMD-160, và được dành cho các ứng dụng của các hàm băm mà đòi hỏi một kết quả hash lâu hơn mà không cần một mức độ bảo mật lớn hơn.

CHƯƠNG 4: XÂY DỰNG THUẬT TOÁN HÀM BĂM

4.1 Phát biểu bài toàn

4.1.1 Vấn đề đặt ra

Khi ta đăng ký một địa chỉ nào đó, internet sẽ yêu cầu đăng ký password. Khi đó internet sẽ không lưu trực tiếp password mà sẽ lưu giá trị hàm băm nào đó vào CSDL. Sau đó, mỗi khi truy cập vào địa chỉ internet, internet sẽ yêu cầu gõ vào password đã đăng ký lần trước, sau đó internet sẽ "băm" password vừa gõ vào máy nếu kết quả băm mà trùng khớp với giá trị băm đã đăng ký thì internet chấp nhận và bạn được tiếp tục sử dụng địa chỉ và nếu trái lại thì internet thông báo là password vừa đưa vào là không đúng và yêu cầu truy cập lại.

Giả sử ta có một password: thidualayeunuoc. Bây giờ dùng hàm băm rồi băm x để nhận được giá trị băm là m = m1,m2,…,m10 trong đó mi = 0 hoặc 1.

4.1.2 Cách tiếp cận và giải pháp

- INPUT: Thông điệp (văn bản) có độ dài tối đa 50 ký tự
- OUTPUT: Bản băm, đại diện cho thông điệp gốc, độ dài cố định.

Tạo một bảng để dán từng kí tự của password với m = m[1] m[2] … m[10] và n = n[1] n[2]…n[5] cho đến khi kết thúc.

	m1	m2	m3	m4	m5	m6	m7	m8	m9	m10
n1	t	h	i	d	u	a	l	a	y	e
n2	u	n	u	o	c	t	h	i	d	u
n3	a	l	a	y	e	u	n	u	o	c
n4	t	h	i	d	u	a	l	a	y	e
n5	u	n	u	o	c	t	h	i	d	u

Gán các kí tự của bảng chữ cái tương ứng với số 0 đến 25

a	0	n	13
b	1	o	14
c	2	p	15
d	3	q	16
e	4	r	17
f	5	s	18
g	6	t	19
h	7	u	20
i	8	v	21
j	9	w	22
k	10	x	23
l	11	y	24
m	12	z	25

Trong đó m[i] là xâu bit có độ dài 10 ký tự, gọi là word; m ≡ 0 mod 26.

M được xây dựng bằng thuật toán:

m[1],[2]…[10] = (n1/m[1],[2]…[10] + n2/ m[1],[2]…[10] + n3/ m[1],[2]…[10] + n4/ m[1],[2]…[10] + n5/ m[1],[2]…[10]) mod 26

Giả sử password: thidualayeunuoc chúng ta sẽ sẽ băm bằng thuật toán:

m1 = (19 + 20 + 0 + 19 + 20) mod 26 = 0 => a

m2 = (7 + 13 + 11 + 7 + 13) mod 26 = 25 => z

m3= (8 + 20 + 0 + 8 + 20) mod 26 = 4 => e

m4= (3 + 14 + 24 + 3 + 14) mod 26 = 6 => g

m5= (20 + 2 + 4 + 20 + 2) mod 26 = 22 => w

m6= (0 + 19 + 20 + 0 + 19) mod 26 = 6 => g

m7= (11 + 7 + 13 + 11 + 7) mod 26 = 23 => x

m8= (0 + 8 + 20 + 0 + 8) mod 26 = 10 => k

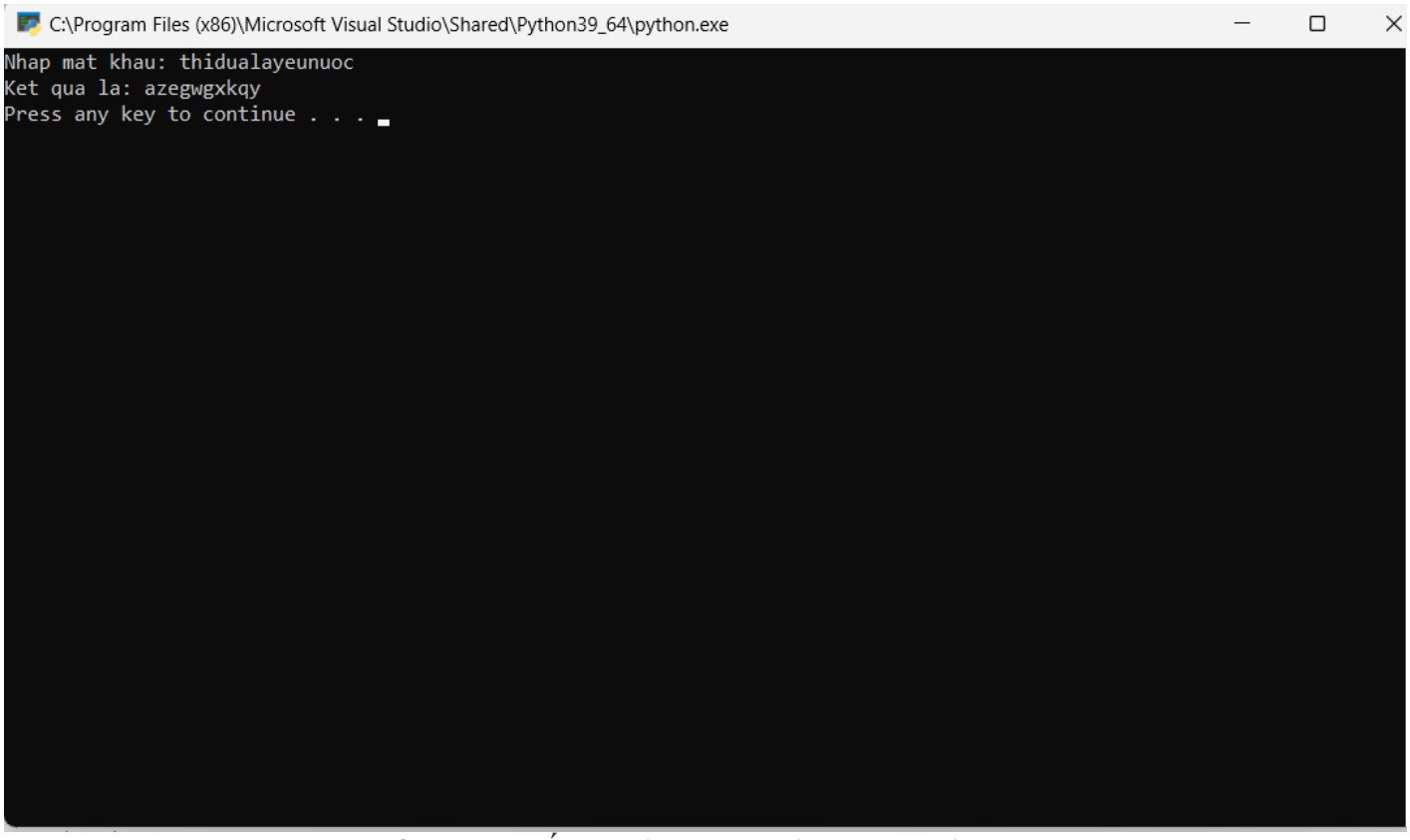
m9= (24 + 3 + 14 + 24 + 3) mod 26 = 16 => q

m10= (4 + 20 + 2 + 4 + 20) mod 26 = 24 => y

Suy ra chúng ta sẽ được đoạn băm password thidualayeunuoc sẽ là : azegwgxkqy

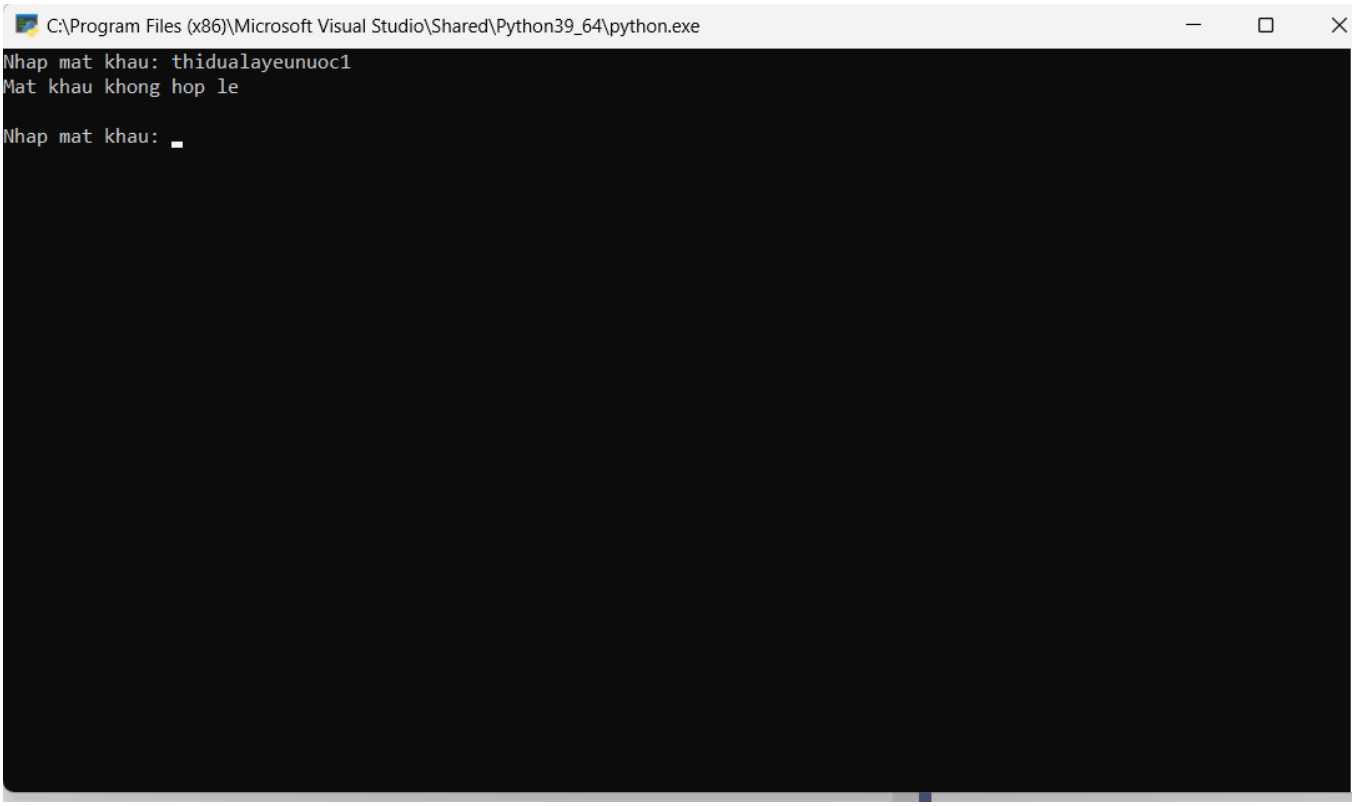
4.1.3 Chạy chương trình cài đặt

Kết quả chương trình:



Hình 4-1 Kết quả băm của chương trình

Nếu password có những kí tự hay số thì chương trình sẽ báo lỗi :



Hình 4-2 Kết quả báo lỗi của chương trình

4.1.4 Mã nguồn chương trình :

```
def table_filling(passwd):
        if len(passwd) > 50 or len(passwd) < 1:
                return None
        letter_positions = []
        for c in passwd:
                num = ord(c) - 97
                if num < 0 or num > 25:
                        return None
                letter_positions.append(num)
        return (letter_positions*50)[:50]

if __name__ == '__main__':
        while True:
                passwd = input("Nhap mat khau: ")
                table = table_filling(passwd)
                if table is None:
                        print("Mat khau khong hop le\n")
                        continue
                else:
                        result = ""
                        for col in range(10):
        c = sum([table[row*10+col] for row in range(5)])
                                        c = c%26
                                        result += chr(c+97)
                        print(f"Ket qua la: {result}")
                        break
```

KẾT LUẬN

Trong đồ án em đã nghiên cứu về hàm băm Ripemd và ứng dụng trong chữ ký số.

Em đã cố gắng nghiên cứu sử dụng tài liệu kết hợp với kiến thức đã được học. Em đã hiểu về an toàn bảo mật mạng, hàm băm và sử dụng công cụ trong việc băm các đoạn văn bản và chữ ký số. Tuy nhiên do thời gian và khả năng còn hạn chế, nên em vẫn chưa tìm hiểu kĩ về các hàm băm khác.

Trong thời gian tới em sẽ tiếp tục và nghiên cứu sâu hơn về các hàm băm MD4,MD5,SHA để có thể sử dụng công cụ trong việc bảo mật

Em xin chân thành cảm ơn.

TÀI LIỆU THAM KHẢO

[1] Bảo mật trên mạng, Bí quyết và giải pháp, NXB Thống kê, 3/2000

[2] Một số hình thức tấn công mạng phổ biến, Bkav security

[3] Thái Hồng Nhị, An toàn thông tin mạng máy tính, truyền tin số và truyền dữ liệu, NXB Khoa học và kỹ thuật.

[4] Dương Thanh Tuấn, Tìm hiểu kỹ thuật phòng thủ mạng, 2014.