THUẬT NGỮ

A

An ninh mạng (Network security)

Các phương tiện để bảo vệ, chống, phát hiện, và hiệu chỉnh các phá hoại an ninh khi truyền và lưu trữ thông tin.

An toàn không điều kiện

ở đây không quan trọng máy tính mạnh như thế nào, có thể thực hiện được bao nhiêu phép toán trong một giây, mã hoá không thể bị bẻ, vì bản mã không cung cấp đủ thông tin để xác định duy nhất bản rõ. Việc dùng bộ đệm ngẫu nhiên một lần để mã dòng cho dữ liệu mà ta sẽ xét cuối bài này được coi là an toàn không điều kiện. Ngoài ra chưa có thuật toán mã hóa nào được coi là an toàn không điều kiện.

An toàn tính toán

với nguồn lực máy tính giới hạn và thời gian có hạn (chẳng hạn thời gian tính toán không quá tuổi của vũ trụ) mã hoá coi như không thể bị bẻ. Trong trường hợp này coi như mã hóa an toàn về mặt tính toán. Nói chung từ nay về sau, một thuật toán mã hóa mà an toàn tính toán, được coi là an toàn.

An toàn thư điện tử

nhằm đảm bảo các yêu cầu sau tính bảo mật nội dung tin gửi, xác thực người gửi mẩu tin, tính toàn vẹn của mẩu tin, hơn nữa bảo vệ khỏi bị sửa, tính chống từ chối gốc, chống từ chối của người nhận.

B

Bài toán Logarit rời rạc: Tìm số mũ để lũy thừa theo cơ số số thứ nhất theo modulo số thứ hai bằng một số cho trước. Đây là bài toán khó, không phải bao giờ cũng có nghiệm.

Bản rõ

là bản tin gốc. Bản rõ có thể được chia nhỏ để có kích thước phù hợp.

Bản mã

là bản tin gốc đã được mã hoá. Ở đây ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.

Bao bọc tải trọng bảo mật ESP:

đảm bảo bảo mật nội dung mẩu tin và luồng vận chuyển giới hạn, có lựa chọn cung cấp dịch vụ xác thực như AH và hỗ trợ phạm vi rộng các mã, các chế độ mã và bộ đệm.

Bảo mật (Confidentiality)

Bảo vệ dữ liệu không bị khám phá bởi người không có quyền. Chẳng hạn như dùng các ký hiệu khác để thay thế các ký hiệu trong bản tin, mà chỉ người có bản quyền mới có thể khôi phục nguyên bản của nó.

Bom logic

đây là một trong những phần mềm có hại kiểu cổ, code được nhúng trong chương trình hợp pháp.

Bức tường lửa (Firewall)

là điểm cổ chai để kiểm soát và theo dõi các gói tin ra vào một mạng con. Các mạng liên kết với độ tin cậy khác nhau, buộc có hạn chế trên các dịch vụ của mạng như vận chuyển phải có giấy phép. Nó kiểm tra và kiểm soát truy cập, có thể cài đặt cảnh báo các hành vi bất thường và cung cấp bảng NAT và sử dụng theo dõi giám sát.

Bức tường lửa lọc gói

là thành phần của bức tường lửa đơn giản nhất và cơ sở của mọi hệ thống tường lửa. Nó kiểm tra mỗi gói IP không có ngữ cảnh và cho phép hay từ chối tùy theo qui tắc xác định. Suy ra có hạn chế truy cập đến các dịch vụ và các cổng.

C

Căn nguyên tố của một số

là số nguyên tố cùng nhau với số đã cho mà lũy thừa của nó tạo nên tập tất cả các số

nguyên tố cùng nhau với số đó và nhỏ hơn nó.

Cơ chế an ninh (Security mechanism)

Từ các công việc thực tế để chống lại các phá hoại an ninh, người ta đã hệ thống và sắp xếp lại tạo thành các cơ chế an ninh khác nhau. Đây là cơ chế được thiết kế để phát hiện, bảo vệ hoặc khôi phục do tấn công phá hoại.

Cơ chế an ninh chuyên dụng

Là cơ chế an ninh được cài đặt trong một giao thức của một tầng mạng nào đó: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, đệm truyền, kiểm soát định hướng và chứng nhận.

Cơ chế an ninh phổ dụng

Là cơ chế an ninh không chỉ rõ được dùng cho giao thức trên tầng nào hoặc dịch vụ an ninh cụ thể nào mà cung cấp chức năng tin cậy cho một tiêu chuẩn nào đó, nhãn an ninh chứng tỏ đối tượng có tính chất nhất định, phát hiện sự kiện, vết theo dõi an ninh, khôi phục an ninh.

Chống từ chối (Nonrepudiation)

Chống lại việc chối bỏ của một trong các bên tham gia trao đổi. Người gửi cũng không trối bỏ là mình đã gửi thông tin với nội dung như vậy và người nhận không thể từ chối được là tôi chưa nhận được thông tin đó. Điều này là rất cần thiết trong việc trao đổi, thỏa thuận thông tin hàng ngày.

Chữ ký điện tử
được xem như thông tin có kích thước cố định phụ thuộc vào bản băm của mẩu tin và một số thông tin của người ký, lần ký. Nó cung cấp các khả năng để kiểm chứng tác giả, ngày và giờ ký, xác thực nội dung mẩu tin và được kiểm chứng bởi bên thứ 3 để chống từ chối. Thường dùng chữ ký điện tử RSA hoặc chuẩn chữ ký điện tử DSS

Chủ quyền khóa công khai
Người có thẩm quyền quản trị và cung cấp khóa công khai trực tuyến, dùng mã khóa riêng ký nhận khóa công khai của người sử dụng

Chủ quyền Giấy chứng nhận
người có thẩm quyền quản trị khóa công khai và cung cấp Giấy chứng nhận khóa công khai của người sử dụng được ký bằng mã khóa riêng

Chữ ký điện tử RSA
là bản mã khóa riêng của người gửi trên bản băm của thông điệp.

Chữ ký điện tử DSA
đây là chuẩn chữ ký điện tử nhanh hơn và an toàn hơn chữ ký RSA, có thuật toán tạo chữ ký cho người gửi và kiểm tra chữ ký cho người nhận.

Chữ ký kép:
Chúng ta có hai thông tin liên quan chặt chẽ với nhau là đơn mua hàng và hóa đơn thanh toán nhưng lại gửi cho hai đối tác khác nhau là người bán và Tổ chức thanh toán. Mà lại không cho các bên biết các thông tin không cần thiết, người bán không biết thông tin về thẻ thanh toán, Tổ chức thanh toán không biết thông tin về hàng hóa đã mua. Để giải quyết vấn đề đó người ta tạo ra chữ ký kép.

Cơ sở thông tin quản trị (MIB)

là cơ sở dữ liệu về các đối tượng với các thuộc tính của chúng để quản trị các nguồn lực trong mạng. Mỗi nguồn lực được thể hiện như một đối tượng. Mỗi đối tượng như một biến dữ liệu biểu diễn một khía cạnh của tác tử quản trị.

Cửa sau hoặc cửa sập

điểm vào chương trình bí mật, cho phép những người biết truy cập mà bỏ qua các thủ tục an toàn thông thường. Kỹ thuật này có

thể được sử dụng chung bởi những người phát triển và là mối đe doạ khi để trong chương trình sản phẩm

D

Dịch vụ an ninh (Security services)

Đây là các công cụ đảm bảo an ninh của hệ thống xử lý thông tin và truyền thông tin trong tổ chức. Chúng được thiết lập để chống lại các tấn công phá hoại. Có thể dùng một hay nhiều cơ chế an toàn để cung cấp dịch vụ.

DSS

Chuẩn chữ ký điện tử, được chính phủ Mỹ ủng hộ từ sơ đồ chữ ký điện tử FIPS 186. Sử dụng thuật toán hash SHA và thuật toán DSS. Tạo 320 bit chữ ký và độ an toàn 512-1024 bit, an toàn phụ thuộc vào độ khó của bài toán logarit rời rạc.

Dịch vụ xác thực X.509

là một phần của chuẩn dịch vụ thư mục X.500. Ở đây các máy chủ phân tán bảo trì cơ sở dữ liệu thông tin của người sử dụng và xác định khung cho các dịch vụ xác thực. Thư mục chứa các chứng nhận khoá công khai, khoá công khai của người sử dụng được ký bởi chủ quyền chứng nhận. Dịch vụ cũng thiết lập các thủ tục xác thực, sử dụng mã khoá công khai và chữ ký điện tử.

Đ

Định lý phần dư Trung hoa

dùng để đưa việc tính toán số học Modulo theo số lớn về việc tính toán số học modulo theo số nhỏ, nếu có thể phân tích số lớn thành tích các số nhỏ nguyên tố cùng nhau. Định lý này cũng giúp giải hệ phương trình modulo.

G

Giả mạo (Masquerade)

Là một thực thể tấn công trong khi giả danh một thực thể khác. Tấn công giả mạo thường được kết hợp với các dạng tấn công khác như tấn công chuyển tiếp và tấn công sửa đổi thông báo.

Giải mã chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hóa.

Giao thức "bản ghi"

xác định khuôn dạng cho tiến hành mã hóa và truyền tin hai chiều giữa hai đối tượng đó. Giao thức SSL "bắt tay" sẽ sử dụng SSL "bản ghi" để trao đổi một số thông tin giữa máy chủ và máy trạm vào lần đầu tiên thiết lập kết nối SSL.

Giao thức "bắt tay"

xác thực các bên tham gia và xác định các tham số giao dịch giữa hai đối tượng có nhu cầu trao đổi thông tin hoặc dữ liệu.

Giao thức quản trị mạng cơ bản SNMP

là giao thức được sử dụng để quản trị mạng TCP/IP. Nó bao gồm các khả năng chính sau: Get cho phép trạm quản trị nhận giá trị của đối tượng tại tác tử, Set cho phép trạm quản trị đặt giá trị của đối tượng tại tác tử, Notify cho phép tác tử nhắc nhở trạm quản trị về một sự kiện quan trọng

H

Hai số nguyên tố

cùng nhau là hai số có ước chung lớn nhất bằng 1. Dùng thuật toán Euclid để kiểm tra hai số có nguyên tố cùng nhau không.

Hàm canh cổng

Biện pháp phát hiện và ngăn chặn các truy cập trái phép thông qua các tiêu chuẩn lọc

Hạ tầng khóa công khai PKI

hệ thống cung cấp và quản lý Giấy chứng nhận về khóa công khai của người sử dụng
Nhiệm vụ của PKI:

- Quản lý danh tính người sử dụng (NSD) với khóa công khai của người đó.
- Cấp chứng nhận của Chủ quyền Giấy chứng nhận CA cho NSD
- Huỷ và Thu hồi các giấy chứng nhận không còn hiệu lực
- Tạo ra các Thư mục để lưu trữ các chứng nhận và danh sách thu hồi (CRL).

- Cung cấp dịch vụ sẵn sàng cung cấp cho NSD như: đăng ký, truy cập, xin giấy chứng nhận, đưa ra danh sách thu hồi CRL

Hash - băm
nén mẩu tin bất kỳ về kích thước cố định. Giả thiết là hàm hash là công khai và không dùng khoá. Hash chỉ phụ thuộc mẩu tin. Hash được sử dụng để phát hiện thay đổi của mẩu tin. Hash có thể sử dụng nhiều cách khác nhau với mẩu tin, Hash thường được kết hợp dùng để tạo chữ ký trên mẩu tin.

Hàm băm SHA: Hàm băm an toàn với đầu vào văn bản chia khối 512 bit, xử lý 4 vòng, mỗi vòng 20 bước với hàm logic và các tham số khác nhau và đầu ra là bản băm 160 bit.
Hàm Euler của một số tự nhiên bằng số các số nguyên tố cùng nhau với nó và nhỏ hơn nó
Hệ thống quản trị mạng
là tập hợp các công cụ để theo dõi và kiểm soát được tích hợp theo nghĩa sau: giao diện thao tác duy nhất với tập các lệnh đủ mạnh và thân thiện để thực hiện hầu hết các nhiệm vụ quản trị mạng; có số tối thiểu các các thiết bị riêng rẽ, hầu hết phần cứng và phần mềm đòi hỏi cho quản trị mạng đều tích hợp vào các thiết bị đã có của người dùng

I

IPSec
là cơ chế an ninh IP tổng quan. Nó cung cấp: xác thực, bảo mật và quản trị khoá. IPSec được dùng trên mạng LAN, mạng WAN riêng và chung và trên cả mạng Internet.

K

Kerberos:

Hệ thống máy chủ xác thực và cung cấp các dịch vụ phân tán được phát triển ở MIT.

Kiểm soát quyền truy cập

Biện pháp để ngăn cấm việc sử dụng nguồn thông tin không đúng vai trò. Mỗi đối tượng trong hệ thống được cung cấp các quyền hạn nhất định và chỉ được hành động trong khuôn khổ các quyền hạn đó.

Khoá
là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khóa là độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
Khóa chính (master key)
khóa dùng để mã các khóa phiên, chia sẻ giữa người sử dụng và trung tâm phân phối khóa.
Khoá công khai
mọi người đều biết, được dùng để mã hoá mẩu tin và kiểm chứng chữ ký.
Khóa phiên (section key)
khóa tạm thời, dùng để mã hoá dữ liệu giữa nhóm người sử dụng cho một phiên logic và sau đó bỏ đi.
Khoá riêng
chỉ người sở hữu biết, đề giải mã bản tin hoặc để tạo chữ ký.

Khuếch tán
là làm tan biến cấu trúc thống kê của bản rõ trên bản mã. Điều đó đạt được nếu mỗi bit của bản rõ tác động đến giá trị của rất nhiều bit trên bản mã hay mỗi bit của bản mã chịu tác động của nhiều bit bản rõ.

L

Liên kết an toàn SA:
đây là quan hệ một chiều giữa người gửi và người nhận mà cung cấp dịch vụ an ninh cho luồng vận chuyển và được xác định bởi 3 tham số

- Chỉ số các tham số bảo mật (SPI): là xâu bit gắn với liên kết, nó cho phép hệ thống nhận tin lựa chọn liên kết để xử lý.
- Địa chỉ IP đích
- Định danh giao thức bảo mật: chỉ rõ liên kết là AH hay ESP.

Logarit rời rạc theo modulo n
là bài toán ngược của bài toán lũy thừa, nhưng khó hơn nhiều, thường đòi hỏi cơ số là căn nguyên tố của n và số lấy logarit cũng là nguyên tố cùng nhau với n.

Lý thuyết mã
bao gồm cả mật mã và thám mã. Nó là một thể thống nhất, để đánh giá một mã mạnh hay không, đều phải xét từ cả hai khía cạnh đó. Các nhà khoa học mong muốn tìm ra các mô hình mã hóa khái quát cao đáp ứng nhiều chính sách an ninh khác nhau.

M

Mã
là thuật toán E chuyển bản rõ thành bản mã. Thông thường chúng ta cần thuật toán mã hóa mạnh, cho dù kẻ thù biết được thuật toán, nhưng không biết thông tin về khóa, cũng không tìm được bản rõ.

Mã dòng
xử lý bản tin theo từng bít hoặc byte, lần lượt mỗi bít hoặc byte được mã hoá hoặc giải mã.

Mã khối
xử lý bản tin theo từng khối, lần lượt mỗi khối được mã hoặc giải mã. Có thể xem giống như phép thế với các ký tự lớn – mỗi khối gồm 64 bít hoặc nhiều hơn.

Mã hoá
là quá trình chuyển bản rõ thành bản mã, thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.

Mã thay thế

là phương pháp mà từng kí tự (nhóm kí tự) trong bản rõ được thay thế bằng một kí tự (một nhóm kí tự) khác để tạo ra bản mã. Bên nhận chỉ cần thay thế ngược lại trên bản mã để có được bản rõ ban đầu.

Mã hoán vị

các kí tự trong bản rõ vẫn được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra bản mã. Tức là các kí tự trong bản rõ hoàn toàn không bị thay đổi bằng kí tự khác mà chỉ đảo chỗ của chúng để tạo thành bản mã.

Mật mã

là chuyên ngành khoa học của Khoa học máy tính nghiên cứu về các nguyên lý và phương pháp mã hoá. Hiện nay người ta đưa ra nhiều chuẩn an ninh cho các lĩnh vực khác nhau của công nghệ thông tin

Mã khoá đối xứng

còn được gọi là mã khoá đơn hay mật. Ở đây chỉ dùng một khoá, dùng chung cả người nhận và người gửi. Khi khoá này được dùng, việc trao đổi thông tin về khoá sẽ được thỏa thuận trước.

Mã khoá công khai

ra đời vào đầu những năm 1970. Có thể nói đây là bước tiến quan trọng nhất trong lịch sử 3000 năm mã hoá. Ở đây người ta sử dụng 2 khoá: một khoá riêng và một khoá công khai. Hai khoá này khác nhau, không đối xứng với nhau, do đó mã khoá công khai, còn được gọi là mã không đối xứng.

Mã xác thực thông điệp:
Sinh ra bởi một thuật toán mà tạo ra một khối thông tin nhỏ có kích thước cố định: phụ thuộc vào cả mẩu tin và khoá nào đó, giống như mã nhưng không cần phải giải mã, bổ sung vào mẩu tin như chữ ký để gửi kèm theo làm bằng chứng xác thực.

Mã xác thực thông điệp:
Sinh ra bởi một thuật toán mà tạo ra một khối thông tin nhỏ có kích thước cố định: phụ thuộc vào cả mẩu tin và khoá nào đó, giống như mã nhưng không cần phải giải mã, bổ sung vào mẩu tin như chữ ký để gửi kèm theo làm bằng chứng xác thực.

Mô hình quản trị mạng SNMP

bao gồm những thành phần chính sau: Trạm quản trị, Tác tử quản trị, Cơ sở thông tin quản trị (MIB), Giao thức quản trị mạng SNMP.

N

Ngựa thành Tơ roa

chương trình với các tác động phụ được dấu kín, mà thông thường rất hấp dẫn như trò chơi hoặc phần mềm nâng cấp. Khi chạy thực hiện những nhiệm vụ bổ sung, cho phép kẻ tấn công gián tiếp dành quyền truy cập mà họ không thể trực tiếp. Thông thường sử dụng lan truyền virus/sâu (worm) hoặc cài đặt cửa sau hoặc đơn giản phá hoại dữ liệu.

R

Rối loạn

là làm cho quan hệ giữa bản mã và khoá càng phức tạp càng tốt. Bản mã có tính rối loạn cao sẽ làm cho việc tìm mò khoá trở nên rất khó khăn, ngay cả khi kẻ tấn công có các đặc trưng thống kê của bản mã và biết cách khoá tác động đến bản mã.

RSA

là mã công khai được sáng tạo bởi Rivest, Shamir & Adleman ở MIT (Trường Đại học Công nghệ Massachusetts) vào năm 1977. RSA là mã công khai được biết đến nhiều nhất và sử dụng rộng rãi nhất hiện nay. Nó dựa trên các phép toán lũy thừa trong trường hữu hạn các số nguyên theo modulo nguyên tố.

P

Phân phối khóa công khai:

cung cấp khóa công khai của người sử dụng một cách an toàn

Q

Quản trị tác tử

Gồm các thiết bị chính như: máy chủ, bridges, routers và hubs có thể được trang bị SNMP, sao cho chúng có thể được điều khiển từ trạm quản trị. Các tác tử được quản trị đáp ứng các yêu cầu về lấy thông tin và truyền hành động từ trạm.

Quyền truy cập

Ngăn cấm việc sử dụng nguồn thông tin không đúng vai trò. Mỗi đối tượng trong hệ thống được cung cấp các quyền hạn nhất định và chỉ được hành động trong khuôn khổ các quyền hạn đó.

S

Sâu

là chương trình tự sinh lặp và gửi các bản sao lan truyền trên mạng từ hệ thống này sang hệ thống khác. Khi đến nơi mới nó có thể tự kích hoạt sinh tiếp và lan truyền. Nó thực hiện các hành động phá hoại.

Số nguyên tố

là số chỉ ước là 1 và chính nó. Muốn phân tích một số ra tích lũy thừa của các thừa số nguyên tố, ta phải xét tính chia hết của nó và các thương nhận được cho từng số nguyên tố từ nhỏ đến lớn

SHA

thuật toán băm an toàn (Secure Hash Algorithm). SHA có nguồn gốc từ Viện chuẩn công nghệ quốc gia Hoa kỳ - NIST & NSA vào năm 1993, sau đó được nâng cấp vào 1995 theo chuẩn US và chuẩn là FIPS 180-1 1995 và Internet RFC3174. Nó được sử dụng với sơ đồ chữ ký điện tử DSA. Thuật toán là SHA dựa trên thiết kế MD4 với một số khác biệt tạo nên giá trị Hash 160 bit.

SSL

là dịch vụ an toàn tầng vận chuyển, ban đầu được phát triển bởi Netscape. Sau đó phiên bản 3 của nó được thiết kế cho đầu vào công cộng và trở thành chuẩn Internet, được biết đến như an toàn tầng vận chuyển TLS (Transport Layer Security). Giao thức SSL hoạt động dựa trên hai nhóm con giao thức là giao thức "bắt tay" và giao thức "bản ghi".

T

Tấn công lặp

là tấn công mà ở đó dịch vụ có chủ quyền đã được thực hiện xong, nhưng bị giả mạo bởi yêu cầu lặp khác để tìm cách sử dụng lại những lệnh có chủ quyền.

Tấn công từ chối dịch vụ

là tấn công làm cho hệ thống trở nên không sẵn sàng, làm tràn bởi sự vận chuyển và thực hiện những việc vô ích. Kẻ tấn công thường sử dụng một số lớn các "zombies" để tăng độ khó của các tấn công.

Tính sẵn sàng (Availability)

Tính chất của hệ thống luôn có thể được truy cập và phục vụ cho các thực thể có quyền, không bị giảm hoặc mất khả năng làm việc.

Thám mã
nghiên cứu các nguyên lý và phương pháp giải mã mà không biết khoá. Thông thường khi đưa các mã mạnh ra làm chuẩn dùng chung giữa các người sử dụng, các mã đó đã được các kẻ thám mã cũng như những người phát triển mã tìm hiểu nghiên cứu kỹ về các phương pháp giải một phần bản mã với các thông tin không đầy đủ.

Thanh toán điện tử an toàn:
là tập các giao thức và định dạng an toàn dùng để trao đổi an toàn giữa các đối tác, tin tưởng vì sử dụng giấy chứng nhận X509v3, riêng biệt vì hạn chế thông tin vừa đủ cho những người tham gia giao dịch.

Thủ tục Diffie – Hellman: trao đổi công khai trên môi trường mạng khóa mật dùng chung giữa hai người sử dụng mà không cần bên thứ ba

Thuật toán bình phương và nhân liên tiếp
là thuật toán tính lũy thừa của một cơ số bằng cách thực hiện liên tiếp việc bình phương và nhân hoặc không nhân với cơ số tùy theo biểu diễn theo cơ số 2 của lũy thừa đó.

Thuật toán Euclid
để tính ước chung lớn nhất của 2 số. Nó lặp việc thay số bằng cặp số nhỏ và phần dư của số lớn theo số nhỏ, cho đến khi 1 số bằng 0, thì số kia là Ước chung lớn nhất.

Thuật toán Euclid mở rộng
tính ước chung lớn nhất và tính nghịch đảo trong trường hợp 2 số nguyên tố cùng nhau. Nó giống như tiến hành đồng thời nhiều thuật toán Euclid cùng một lúc

Thư mục công cộng:

Thư mục có người quản trị để mọi người sử dụng đăng ký và chia sẻ khóa công khai

Tiêu đề xác thực AH
cung cấp sự hỗ trợ cho toàn vẹn dữ liệu và xác thực của các gói IP; hệ thống đầu cuối/chuyển mạch có thể xác thực người sử dụng/ứng dụng; ngăn tấn công theo dõi địa chỉ bằng việc theo dõi các chỉ số dãy và chống tấn công tải lại.

Toàn vẹn dữ liệu (Data Integrity)

Bằng chứng để tin tưởng là dữ liệu được gửi từ người có quyền. Nếu có thay đổi như làm trì hoãn về mặt thời gian hay sửa đổi thông tin, thì bằng việc xác thực sẽ cho cách kiểm tra nhận biết là có các hiện tượng đó đã xảy ra hay không.

Tổ chức thanh toán:
tổ chức tài chính thực hiện việc chuyển tiền từ thẻ thanh toán của người mua sang tài khoản của người bán. Thông thường người bán chấp nhận nhiều loại thẻ của nhiều ngân hàng khác nhau. Tổ chức thanh toán là trung gian được các ngân hàng và người bán ủy quyền.

Trao đổi khoá Diffie Hellman
là sơ đồ khoá công khai đầu tiên được đề xuất bởi Diffie và Hellman năm 1976 cùng với khái niệm khoá công khai. Sau này được biết đến bởi James Ellis (Anh), người đã đề xuất bí mật năm 1970 mô hình tương tự. Đây là phương pháp thực tế trao đổi công khai các khoá mật đối xứng.

Trạm quản trị

là thiết bị đứng tách rời hoặc cài đặt trên hệ thống chia sẻ. Trạm quản trị phục vụ như giao diện cho người quản trị mạng kết nối vào hệ thống quản trị mạng. Trạm có tối thiểu: tập các ứng dụng quản trị để phân tích dữ liệu, khắc phục lỗi, giao diện có khả năng theo dõi và kiểm soát các thành phần ở xa trong mạng và cơ sở dữ liệu thông tin được lấy từ các thực thể được quản trị trên mạng

V

Virus

là đoạn code tự sinh lặp đính kèm với code khác như virus sinh học. Nó tự lan truyền mang theo code để tạo các bản sao của chính nó. Và nó cũng thực hiện nhiệm vụ ngầm nào đó như phá hoại các files hệ thống.

X

Xác thực

Xác thực một đối tượng còn có nghĩa là công nhận nguồn gốc của đối tượng, trong khi, xác thực một người thường bao gồm việc thẩm tra nhận dạng của họ. Việc xác thực thường phụ thuộc vào một hoặc nhiều nhân tố xác thực để minh chứng cụ thể

Xác thực thực thể

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

Xác thực mẩu tin

liên quan đến các khía cạnh sau khi truyền tin trên mạng

- Bảo vệ tính toàn vẹn của mẩu tin: bảo vệ mẩu tin không bị thay đổi hoặc có các biện pháp phát hiện nếu mẩu tin bị thay đổi trên đường truyền.
- Kiểm chứng danh tính và nguồn gốc: xem xét mẩu tin có đúng do người xưng tên gửi không hay một kẻ mạo danh nào khác gửi.
- Không chối từ bản gốc: trong trường hợp cần thiết, bản thân mẩu tin chứa các thông tin chứng tỏ chỉ có người xưng danh gửi, không một ai khác có thể làm điều đó. Như vậy người gửi không thể từ chối hành động gửi, thời gian gửi và nội dung của mẩu tin.

Y

Z

Zombie

đây là chương trình bí mật điều khiển máy tính của mạng khác và sử dụng nó để gián tiếp tiến hành các tấn công. Thông thường sử dụng để khởi động tấn công từ chối các dịch vụ phân tán (DdoS). Khai thác các lỗ hổng trong các hệ thống.