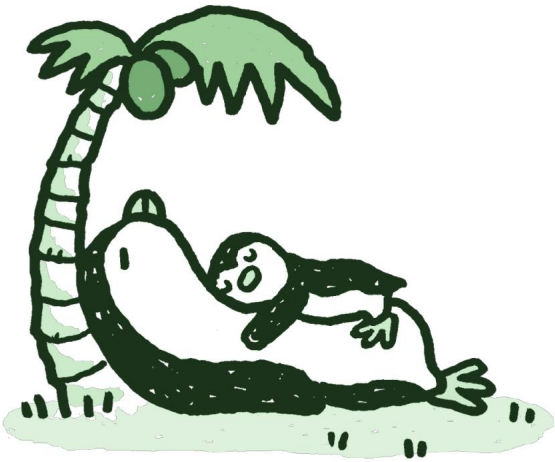
9

Bảo vệ



9.1 Bảo mật thông tin

•Bảo mật thông tin là gì?

Dữ liệu liên hệ được đăng ký trong sổ địa chỉ và khi bạn đăng nhập vào trang web
Mật khẩu, dữ liệu thẻ tín dụng được nhập khi mua sắm trực tuyến
Tất cả những dữ liệu này đều là tài sản thông tin quan trọng và sẽ là một thảm họa nếu chúng bị mất, bị đánh
cắp và sử dụng sai mục đích. Do đó, các biện pháp khác nhau phải được thực hiện để bảo vệ nó. Điều này được gọi
là bảo mật thông tin. Phương tiện bảo mật thông tin
kayousei
Duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của tài sản .

• Bảo mật

Đó là để bảo vệ thông tin khỏi truy cập trái phép và loại bỏ rò rỉ thông tin cho bên thứ ba . ngày
có thể được cải thiện bằng các kỹ thuật như mã hóa dữ liệu.

•Tính đầy

đủ Tính đầy đủ và chính xác không bị viết lại hoặc thiếu sót kể từ thời điểm tạo thông tin
là. Nó có thể được cải thiện bằng các kỹ thuật như chữ ký số.

•Tính khả dụng

Điều đó có nghĩa là tài sản thông tin có thể được sử dụng khi người dùng cần chúng. Được đề xuất để sao lưu thường xuyên, v.v.
có thể được nâng lên.

hình mờ điện tử

Nhúng thông tin vào nội dung số như hình ảnh, âm thanh và video
Công nghệ. Thông tin như tên tác giả, thông tin thanh toán và số lượng bản sao có thể được tạo
Bằng cách nhúng, có thể phân biệt việc sao chép trái phép và làm sai lệch dữ liệu.
có thể làm được.

Bắt đầu với kỳ thi mùa xuân 2014, các kỳ thi buổi sáng sẽ tập trung vào lĩnh vực an toàn thông tin.
Tỷ lệ chủ đề tăng lên. Ngoài ra, trong kỳ thi buổi chiều, cùng một lĩnh vực là một câu hỏi trắc nghiệm?
đã được đổi thành câu hỏi bắt buộc.

Hôm nay

• Các mối đe dọa đối với tài sản thôngtin

Để thực hiện các biện pháp đảm bảo an toàn thông tin, trước hết phải xác định tài sản thông tin bị phơi bày trước những mối đe dọa nào?
Bạn cần biết chính xác những gì bạn đang làm. Các mối đe dọa mà thông tin bị lộ bao gồm:

Jinteki
Có ba loại mối đe dọa : mối đe dọa kỹ thuật, mối đe dọa con người và mối đe dọa vật lý.

•Mối đe dọa kỹ thuật

Các mối đe dọa sử dụng công nghệ máy tính được gọi là các mối đe dọa kỹ thuật. Các mối đe dọa kỹ thuật là lừa đảo
Có nhiều phương pháp và cuộc tấn công khác nhau, bao gồm truy cập và virus máy tính.

·Đánh bắt cá

Tạo một trang web giả vờ là một ngân hàng, v.v. , gửi e-mail có URL,
Một nỗ lực lừa đảo để lừa người dùng giành quyền truy cập vào mã PIN hoặc mật khẩu.
được gọi là ng.

•Đầu độc bộ đệm DNS

Máy chủ DNS do PC tham chiếu được thực hiện để ghi nhớ thông tin quản lý tên miền sai,
Một cuộc tấn công trực tiếp đến một máy chủ được gọi là ngộ độc bộ đệm DNS.

•Tiêm SQL

Nhập lệnh để thực hiện các truy vấn và hoạt động độc hại trên các ứng dụng web
để ngăn chặn các cuộc tấn công làm sai lệch hoặc lấy trái phép dữ liệu cơ sở dữ liệu.
Nó được gọi là tiêm SQL. Để ngăn chặn cuộc tấn công này, các câu bạn đang gõ
các ký tự có ý nghĩa đặc biệt trong các truy vấn và hoạt động cơ sở dữ liệu
Vô hiệu hóa nó để nó không được giải thích.

•D -dos cấp hệ điều hành

Tấn công DoS là một cuộc tấn công gửi một lượng lớn dữ liệu đến máy chủ và khiến máy chủ ngừng hoạt động.

Nó được gọi là một hit.

•Tấn công duyệt thư mục

Nếu bạn chỉ định một tệp trong máy chủ web có đường dẫn không được quản trị viên dự định,

tấn công duyệt thư mục

Nó được gọi là.

•Tín hiệu web

Bằng cách nhúng các hình ảnh nhỏ vào các trang web, v.v., có thể thu được thông tin như xu hướng truy cập của người dùng.

Cơ chế thu thập thông tin được gọi là web beacon.

•Lạm dụng keylogger

Keylogger ban đầu được thiết kế để giám sát đầu vào bàn phím để hỗ trợ người dùng.

Phần mềm để xem và ghi âm. Các phương pháp độc hại như lén lút cài đặt máy tính để thu

thập mật khẩu do người dùng nhập khi sử dụng Internet banking

đươ c dùng như

thuật ngữ

[Hình mờ kỹ thuật số]: Bằng cách nhúng thông tin, bản sao trái phép và dữ liệu

giả mạo dữ liệu

[Lừa đảo]: Đánh cắp thông tin bằng cách khiến người dùng truy cập các trang web giả mạo

[Ngộ độc bộ đệm DNS]: Máy chủ DNS bị lừa ghi nhớ thông tin quản lý tên miền

không chính xác và được chuyển hướng đến máy chủ giả mạo.

[SQL Injection]: Các cuộc tấn công độc hại vào các ứng dụng web

nhập một câu lệnh SQL để thay đổi dữ liệu cơ sở dữ liệu,

đi đúng

[Tấn công DoS]: Dừng chức năng máy chủ bằng cách gửi một lượng lớn dữ liệu

cho phép

[Tấn công duyệt thư mục]: Mật khẩu không được quản trị viên cho phép.

truy cập trái phép vào các tập tin trong máy chủ web

[Web beacon]: Nhúng một hình ảnh nhỏ và thu thập các xu hướng truy cập

thuật ngữ

[Keylogger]: Một máy tính được thiết lập để thu thập mật khẩu đầu vào cho mục đích xấu.

vì

mối đe dọa của con người

Các mối đe dọa do con người gây ra được gọi là mối đe dọa của con người. Máy tính bị đặt sai vị trí hoặc bị xử lý sai

Lỗi vô ý của chủ sở hữu thông tin, chẳng hạn như lỗi sản xuất hoặc lỗi cố ý của người trong cuộc

Điều này bao gồm rò rỉ thông tin cho bên thứ ba.

·Kỹ thuật xã hội

Giả làm quản trị viên hệ thống, v.v., hỏi người dùng và hỏi mật khẩu

, hoặc tiết lộ thông tin bí mật trong một tổ chức dưới chiêu bài khẩn cấp.

Hành động đánh cắp thông tin thông qua lỗ hổng tâm lý được gọi là kỹ thuật xã hội.

•Giả mạo

Sử dụng ID hoặc mật khẩu bị đánh cắp để giả làm người đó trên mạng

Điều này được gọi là giả mạo. Giả mạo đánh cắp thông tin hoặc gây rắc rối

cho người khác.

•Phương pháp salami

Hỗ trợ các phương pháp lừa đảo dần dần một số lượng lớn tài sản đến mức các hoạt động gian lận không xuất hiện.

Nó được gọi là phương pháp Lami.

các mối đe dọa vật lý

Các mối đe dọa vật lý đề cập đến các mối đe dọa gây thiệt hại vật chất cho máy tính và mất thông

tin, chẳng hạn như các thảm họa như mưa lớn, động đất và sét đánh hoặc lỗi máy tính. Trộm cắp

hoặc phá hủy máy tính do trộm cắp cũng được bao gồm trong danh mục này.

thuật ngữ

[Social engineering]: Lợi dụng lỗ hổng trong tâm lý con người

lấy thông tin bí mật

[Phương pháp Salami]: Lừa đảo một số lượng lớn tài sản từng chút một

•Đánh giá rủi ro

Rủi ro

Nó được gọi là. Xác định rủi ro đối với tài sản thông tin và

đánh giá rủi ro

gọi là tổng. Dựa trên số tiền tổn thất và xác suất xảy ra thu được từ phân tích, khi rủi ro xảy ra

Đánh giá mức độ thiệt hại do thảm họa gây ra, sắp xếp thứ tự ưu tiên và xem xét cách ứng phó.

Các biện pháp đối phó rủi ro bao gồm các phương pháp sau.

<Các loại biện pháp đối phó rủi ro>

các loại	nội dung	ví dụ
Lo ngại rủi ro	Để loại bỏ nguyên nhân gây ra rủi ro. Tổn thất lớn Các hành động được thực hiện đối với rủi ro cao	hủy thông tin cá nhân; Đình chỉ xuất bản web, v.v.
Chuyển giao rủi ro (chia sẻ rủi ro)	Để người khác chịu rủi ro. Các biện pháp đối phó với rủi ro có tổn thất lớn và tỷ lệ xảy ra thấp	Đăng ký bảo hiểm, vv
Giảm thiểu rủi ro	Giảm thiểu tổn thất do rủi ro trong phạm vi chấp nhận được. Các biện pháp đối phó rủi ro với tổn thất nhỏ và tỷ lệ xảy ra cao	Mã hóa thông tin, v.v.
Để nguyên một rủi ro mà không thực hiện các biện pháp ngăn ngừa rủi ro .	Các biện pháp đối phó rủi ro với tổn thất nhỏ và tỷ lệ xảy ra nhỏ	

thuật ngữ

[Đánh giá rủi ro]: Đánh giá và phân tích các rủi ro dự đoán.

Ưu tiên ứng phó theo số lượng tổn thất và xác suất xảy ra

kỹ năng

Có thể trả lời về loại rủi ro và từng trường hợp

hãy giữ

•Hệ thống quản lý bảo mật thông tin

Để duy trì bảo mật thông tin, các công ty phải quản lý thông tin đúng cách và giữ bí mật.

Cần phải thiết lập một cơ chế để bảo vệ và liên tục cải tiến nó. cái này

Cơ chế là một hệ thống quản lý bảo mật thông tin hoặc tôi ISMS SMS (Thông tin thông tin

Bảo vệ sự quản lý hệ thống

hệ thống quản lý an ninh).

Quy trình thiết lập ISMS đại khái như sau. (1) Phân tích và đánh
giá rủi ro (2) Lựa chọn
mục tiêu quản lý và biện pháp quản lý để ứng phó với rủi ro
(3) Chuẩn bị tuyên bố áp dụng

kỹ năng

Phân tích Đánh giá Xác định các biện pháp đối phó Tuyên bố quy trình thiết lập ISMS

Hãy nhớ dòng chảy chung của các từ.

•Cách ngăn rò rỉ thông tin

Thông tin bí mật phải được xử lý thích hợp để ngăn chặn rò rỉ thông tin. bê tông
Như một biện pháp đối phó, có các phương pháp sau đây.

• Khi mang các tệp bí mật trong máy tính xách tay

Khi mang các tệp bí mật trong máy tính xách tay, sẽ có nguy cơ bị đánh cắp hoặc mất
mát, vì vậy có thể ngăn chặn rò rỉ thông tin bằng cách mã hóa nội dung của đĩa cứng.

• Khi xử lý các tập tin bí mật

Vứt bỏ máy tính chứa các tệp bí mật bằng cách giao nó cho công ty xử lý chất thải công nghiệp.
xóa hoàn toàn dữ liệu, chẳng hạn như bằng cách ghi đè lên toàn bộ khu vực của đĩa từ nhiều lần.
cần phải làm điều đó.

• Khi gửi các tập tin bí mật qua e-mail

Khi đặt mật khẩu cho hồ sơ mật và đính kèm vào hộp thư điện tử thì mật khẩu đó là
Đừng đưa nó vào email mà hãy gửi nó cho bên kia theo cách khác. sai địa chỉ
Ngay cả khi các tệp bí mật được gửi do nhầm lẫn, việc rò rỉ thông tin vẫn có thể được ngăn chặn.

kỹ năng

Hãy tìm hiểu các phương pháp cụ thể để ngăn chặn rò rỉ thông tin.

試験にチャレンジ

Kỳ thi kỹ sư công nghệ thông tin cơ bản mùa xuân 2015

Điều nào sau đây mô tả một cuộc tấn công SQL injection?

Trả lời: Khi có sự cố với ứng dụng web, truy vấn hoặc thao tác độc hại

Nhập câu lệnh để lấy trái phép hoặc giả mạo dữ liệu trong cơ sở dữ liệu

tấn công

B: Cho phép khách truy cập xem một trang web nhúng tập lệnh độc hại,

Một cuộc tấn công buộc khách truy cập thực hiện các thao tác ngoài ý muốn trên một trang web khác

C: Trở thành máy chủ lưu trữ bằng cách khai thác các lỗ hổng trong DBMS có sẵn trên thị trường

Tìm kiếm máy chủ cơ sở dữ liệu, tự lây nhiễm nhiều lần, buôn bán Internet

Các cuộc tấn công làm tăng lưu lượng truy cập

D: Đối với các trang web hiển thị dữ liệu đầu vào của khách truy cập như trên màn hình,

Một cuộc tấn công khiến trình duyệt của khách truy cập chạy bằng cách gửi dữ liệu

đầu vào nhúng tập lệnh độc hại.

bình luận

SQL injection độc hại trên các ứng dụng web

Nhập câu lệnh SQL để giả mạo và lấy dữ liệu cơ sở dữ liệu trái phép

tấn công. Trả lời: A

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa xuân 2014

Cuộc tấn công nào sau đây đe dọa tính "toàn vẹn" của bảo mật thông tin?

A: Thay đổi trang web

B: Sao chép trái phép dữ liệu được lưu trữ trong hệ thống

C: Tấn công DoS làm quá tải hệ thống

D: Nghe lén nội dung liên lạc

bình luận

Tính toàn vẹn là trạng thái mà thông tin không bị thay đổi hoặc thiếu sót. mạng

Sửa lỗi trang là một cuộc tấn công toàn vẹn. Trả lời: A

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa thu 2013

Điều nào sau đây tương ứng với chia sẻ rủi ro (chuyển giao rủi ro)?

A: Giảm tỷ lệ tổn thất

B: Phân tán rủi ro cho những người khác bằng cách mua bảo hiểm, v.v.

C: Loại bỏ nguyên nhân gây ra rủi ro D: Chia

nhỏ hoặc hợp nhất rủi ro thành các đơn vị có thể quản lý được

bình luận

Chia sẻ rủi ro là chia sẻ và phân tán rủi ro với những người khác.

trả lời: tôi

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa thu 2014

Điều nào sau đây áp dụng cho các biện pháp đối phó rò rỉ thông tin?

A: Thêm tổng kiểm tra vào dữ liệu sẽ được gửi. B: Phản chiếu đĩa

cứng nơi dữ liệu được lưu trữ. C: Lưu trữ một bản sao của phương tiện sao lưu dữ

liệu tại một địa điểm từ xa. D: Mã hóa nội dung của đĩa cứng của máy tính xách tay.

bình luận

Do máy tính xách tay có nguy cơ bị đánh cắp hoặc thất lạc cao nên nội dung của đĩa cứng được

mã hóa để ngăn rò rỉ thông tin. Đáp án: D

9.2 virus máy tính

• Virus máy tính là gì?

Vi-rút máy tính tuân thủ các tiêu chuẩn về biện pháp đối phó với vi-rút máy tính do Bộ Kinh tế, Thương mại và Công nghiệp đặt ra.
được định nghĩa là "một chương trình được thiết kế có chủ ý để gây ra một số loại thiệt hại cho chương
trình hoặc cơ sở dữ liệu của bên thứ ba và có một hoặc nhiều chức năng sau."
được bao gồm.

<Ba chức năng của virus máy tính>

(1) "Chức năng tự lây nhiễm" sao chép chính nó sang các chương trình khác và lây nhiễm chúng

(2) "Chức năng tiềm ẩn" không hiển thị các triệu chứng cho đến một ngày và thời gian cụ thể hoặc số lần được xử lý

(3) "Chức năng trục trặc" làm hỏng tệp hoặc hoạt động ngoài ý muốn của nhà thiết kế

phần mềm độc hại

Trong những năm gần đây, nhiều loại vi-rút không phù hợp với định nghĩa này đã
phần mềm độc hại nói chung đã trở thành phần mềm độc hại.
Tôi gọi nó là a.

• Các loại virus máy tính

Virus máy tính bao gồm:

<Các loại virus máy tính>

các loại	tính năng
Sử dụng chức năng macro của phần mềm xử lý văn bản virus loại macro , phần mềm bảng tính, v.v.	virus để lây nhiễm. Bị lây nhiễm chỉ bằng cách mở một tập tin
Virus lây nhiễm tập tin	Một loại vi-rút lây nhiễm các tệp thực thi có phần mở rộng như com, exe và sys. Bị lây nhiễm do thực thi một chương trình bị lây nhiễm
Loại lây nhiễm khu vực hệ thống vi-rút	Một loại vi-rút lây nhiễm các khu vực hệ thống (chẳng hạn như các khu vực khởi động) được tải đầu tiên khi máy tính khởi động. Bị lây nhiễm khi khởi động máy tính

các loại	tính năng
con ngựa thành trojan	Một loại vi-rút xâm nhập máy tính dưới vỏ bọc của phần mềm thông thường và phá hủy hoặc thay đổi dữ liệu hoặc làm rò rỉ tệp. không tự sao chép
Một loại vi-rút dạng sâu	hoạt động độc lập, xâm nhập vào các máy tính khác thông qua mạng và tự phát tán.

thuật ngữ

[Trojan Horse]: Xâm nhập máy tính dưới vỏ bọc của phần mềm bình thường. Phá hủy hoặc làm sai lệch dữ liệu

• Các biện pháp phòng chống virus máy tính

Về phòng ngừa, phát hiện và xử lý sau khi lây nhiễm virus máy tính,
Tiêu chuẩn chống vi-rút".

•Phòng chống

virus Các nguồn lây nhiễm virus chủ yếu là e-mail và các trang web. bằng email

Để ngăn ngừa lây nhiễm, không mở tệp đính kèm được gửi từ những người không quen biết.

Điều quan trọng là Để ngăn ngừa lây nhiễm khi duyệt các trang web, hãy đảm bảo trình duyệt của bạn có tệp đáng ngờ

Có các biện pháp đối phó như cài đặt không hiển thị các trang web mới. ác quỷ

Ngoài ra, hãy sửa đổi HĐH và các ứng dụng để ngăn ngừa lây nhiễm bằng cách khai thác các lỗ hổng trong PC.

Dán miếng dán đúng cách.

•Phát hiện vi-rút

Đảm bảo cài đặt phần mềm chống vi-rút trên máy tính của bạn. thỏ rừng

Phần mềm diệt vi-rút sử dụng thông tin về vi-rút đã biết (mã chữ ký) làm định nghĩa vi-rút.

Virus được phát hiện và loại bỏ bằng cách so sánh với tệp này.

Giấm. Điều này được gọi là khớp mẫu. Virus mới mỗi ngày

, để nó có thể xử lý các loại vi-rút mới nhất.

Tệp định nghĩa phải được cập nhật thường xuyên.

• Ứng phó sau khi

lây nhiễm Nếu bạn bị nhiễm vi-rút, hãy ngắt kết nối máy tính khỏi mạng ngay lập tức.

Điều quan trọng là phải buông bỏ. Điều này lây lan sự lây nhiễm hơn nữa thông qua mạng.

Điều này là để ngăn chặn thiệt hại lan rộng.

tháo rời

Là một phương pháp hiệu quả để làm sáng tỏ hành vi của các loại virus mới, nghịch đảo

Có tiếng lầm bầm. chuyển đổi từ mã nhị phân sang mã nguồn

Bằng cách đó, chúng tôi sẽ làm sáng tỏ hành vi của loại virus mới.

thuật ngữ

[Phương pháp khớp mẫu]: Thông tin về vi-rút đã biết (mã chữ ký

) được sử dụng để so sánh tệp đích và phát hiện vi-rút

kỹ năng

Ghi nhớ các phương pháp thích hợp để đối phó với vi-rút (phần mềm độc hại)

Đi nào

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa thu 2013

Biện pháp chống phần mềm độc hại nào sau đây phù hợp với PC khách?

A: Để quét vi-rút thủ công thông thường trên PC, phần mềm chống vi-rút

Chỉ nhắm mục tiêu các tệp được tạo sau ngày và giờ khi tệp định nghĩa được cập nhật.

để quét.

B: Để ngăn chặn vi-rút khai thác các lỗ hổng của PC và lây nhiễm

Á p dụng bản vá ứng dụng một cách thích hợp.

C: Để tránh bị nhiễm virus đính kèm trong e-mail, không sử dụng

Cấm giao tiếp với cổng TCP.

d: Để ngăn sâu xâm nhập PC khách, hãy thêm địa chỉ IP toàn cầu động

đưa ra một cuộc đua.

bình luận

Tất cả các tệp phải được quét sau khi cập nhật tệp định nghĩa.

Do đó, A sai. Cấm giao tiếp với các cổng TCP không được sử dụng

Tuy nhiên, không thể kiểm tra nội dung email và ngăn ngừa nhiễm vi-rút.

U cũng sai. Ngay cả khi bạn chỉ định một địa chỉ IP toàn cầu động cho PC khách,

D cũng sai vì không thể ngăn chặn sự xâm nhập của giun. trả lời: tôi

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa thu 2008

Kết hợp các chức năng bất hợp pháp như phá hủy hoặc làm sai lệch dữ liệu vào một phần của chương trình

Cái nào bạn sẽ gửi cho tôi để cài đặt và chạy?

Trả lời: Tấn công DoS

B: Tấn công từ điển

C: Con ngựa thành Troy

D: Tấn công tràn bộ đệm

bình luận

Từ khóa là "các chức năng trái phép như phá hủy và làm sai lệch dữ liệu", "chương trình

Nó được kết hợp như một phần của hệ thống." Đáp án: C

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa thu 2014

Điều nào sau đây mô tả phương pháp khớp mẫu của phần mềm chống vi-rút?

Đ: So sánh tệp trước khi lây nhiễm với tệp sau khi lây nhiễm và

Phát hiện vi-rút bằng cách kiểm tra xem nó có bị hỏng hay không.

B: Phát hiện virus bằng cách so sánh với dấu hiệu của virus đã biết.

C: Bằng cách theo dõi các hiện tượng bất thường do virus gây ra trong hệ thống,

Phát hiện virus.

D: Phát hiện virus bằng cách so sánh với checksum của file.

bình luận

Phương pháp đối sánh mẫu sử dụng thông tin vi-rút đã biết để phát hiện vi-rút

bằng cách so sánh chúng với các tệp mục tiêu. Chữ ký là Câu trả lời của trình

thông tin và mẫu virus máy tính. biên dịch:

9.3 Mã hóa và xác thực

• Mã hóa dữ liệu

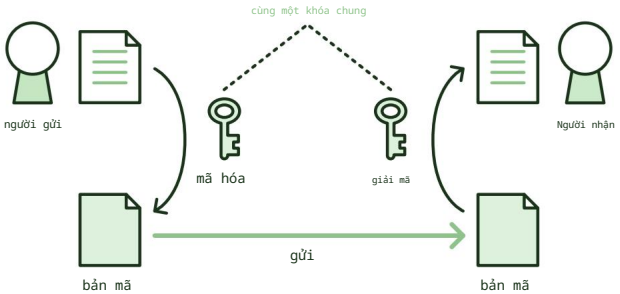
Mã hóa, như tên cho thấy, chuyển đổi dữ liệu thành "bản mã" mà bên thứ ba không thể giải mã được.
trao đổi. Mã hóa bảo vệ dữ liệu của bạn khỏi bị người khác đánh cắp khi đang chuyển tiếp.
Ngay cả khi nó bị đánh cắp, sẽ không ai biết được nội dung của dữ liệu. Khôi phục dữ liệu được mã hóa được
gọi là giải mã .

Mã hóa và giải mã đều sử dụng một khóa để chuyển đổi dữ liệu. Một khóa là một dữ liệu
Dữ liệu đặc biệt để chuyển đổi. Có thể có các lược đồ mã hóa khác nhau do sự khác biệt chính này.
Tôi có.

•Phương pháp mã hóa khóa chung

Một hệ thống mật mã sử dụng cùng một khóa để mã hóa và giải mã được gọi là hệ thống mật mã khóa đối xứng. của dữ liệu
Người gửi và người nhận phải có cùng khóa chung. gửi chìa khóa trước
Nó được phân phối từ người tin tưởng đến người nhận, nhưng nếu chìa khóa bị đánh cắp, bất kỳ ai cũng
có thể giải mã được, vì vậy cần phải cẩn thận khi bàn giao chìa khóa.
Mật mã khóa chung được đặc trưng bởi quá trình mã hóa và giải mã nhanh. nhưng dữ liệu
Vì cần phải tạo bao nhiêu khóa tùy theo số lượng người nhận, nên có thể gửi dữ liệu đến một số lượng người không xác định.
Không thích hợp để gửi.
Các hệ thống mật mã khóa phổ biến bao gồm D ES và AES . đs AES

<Hệ thống mật mã khóa chung>



•Hệ thống mật mã

khóa công khai Hệ thống mật mã sử dụng hai cặp khóa để mã hóa và giải mã

được gọi là mật mã khóa công khai. Người nhận phải nhập khóa công khai được sử dụng để mã hóa trước.

Nó được công khai trên Internet, v.v. và người gửi sử dụng khóa để mã hóa dữ liệu.

Làm. Việc giải mã được thực hiện với khóa riêng do người nhận nắm giữ. khóa công khai

có thể được sử dụng, nhưng khóa riêng phải được giữ bí mật chỉ cho người nhận.

Tôi không.

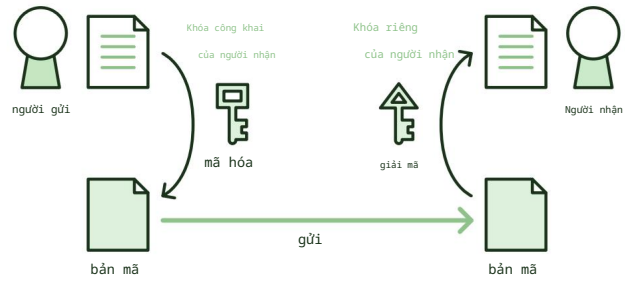
Vì khóa là công khai nên nó phù hợp để nhận dữ liệu từ một số bên không xác định.

Tuy nhiên, nhược điểm là quá trình mã hóa và giải mã mất nhiều thời gian. Các hệ thống

mật mã khóa công khai điển hình sử dụng khó khăn trong việc phân tích thừa số nguyên tố của các số khổng lồ

RSA
I. Có SA và mật mã đường cong elip .

<Hệ thống mật mã khóa công khai>



Trong đề thi, khóa dùng để mã hóa là khóa mã hóa, còn khóa dùng để giải mã

Khóa được gọi là khóa giải mã. Trong mật mã khóa công khai, khóa mã hóa =

Khóa công khai của người nhận, khóa giải mã = khóa riêng của người nhận.

thuật ngữ

[Mật mã khóa chung]: Mã hóa và giải mã bằng cùng một khóa (khóa chung) [Mật

mã khóa công khai]: Mã hóa bằng khóa chung của người nhận và giải mã bằng khóa riêng

LÀM

[RSA]: Mã hóa khóa công khai dựa trên độ khó của việc phân tích thừa số nguyên tố của các số khổng lồ

số hệ thống

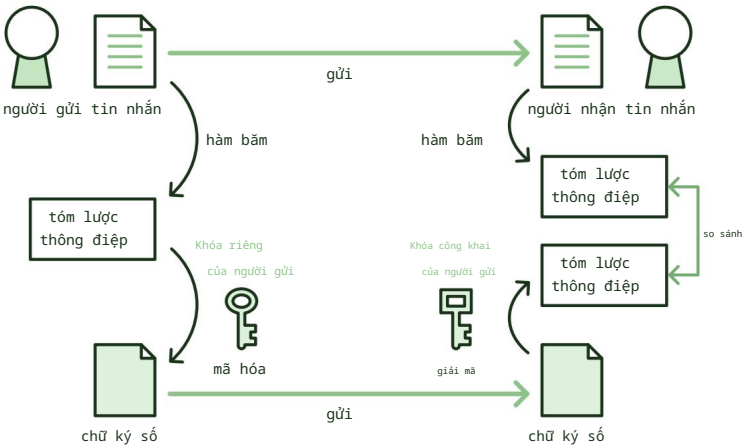
• Chữ ký số

Sử dụng công nghệ áp dụng mật mã khóa công khai, dữ liệu số
Nó có thể được ký để chứng minh rằng đó là dữ liệu. số hóa cái này
gọi là chữ ký. Chữ ký điện tử là một hàm băm ([4-6 Thuật toán tìm kiếm]
) để trích xuất một đoạn dữ liệu cô đọng, được gọi là thông báo tóm tắt, từ thông báo.
Được tạo và mã hóa bằng khóa riêng của bạn.

Người nhận nhận được tin nhắn và chữ ký điện tử. tin nhắn là băm
Một hàm được sử dụng để tạo thông báo tóm tắt và chữ ký số được giải mã bằng khóa công khai của
người gửi để tạo thông báo thông báo.

Nếu các bản tóm tắt thông báo được so sánh và chúng khớp nhau, thì nội dung của thông báo đã bị thay đổi trong quá trình truyền.
Bạn có thể chứng minh rằng nó không bị chỉnh sửa và nó được tạo bởi người gửi.

<Chữ ký số>



Giới thiệu chứng thư số cho điện thoại thông minh

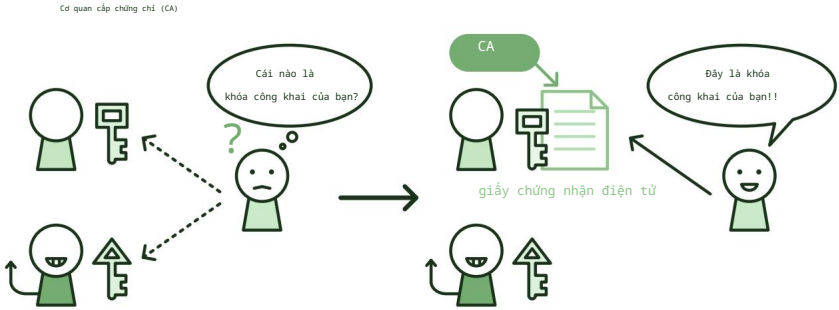
Giới thiệu chứng thư số cho điện thoại thông minh được sử dụng bởi nhân viên
Làm như vậy, khi truy cập vào hệ thống nội bộ, điện thoại thông minh
Bạn có thể xác minh rằng điện thoại của mình là thiết bị mà bạn được phép truy cập.
Giám.

CA

• Cơ quan chứng nhận (MỘT)

Một tổ chức bên thứ ba để chứng minh rằng khóa công khai thực sự thuộc về người đó

Nó được gọi là cơ quan cấp chứng chỉ (CA:C Certification A authority). Cơ quan cấp chứng chỉ là một Chứng chỉ kỹ thuật số được cấp dựa trên ứng dụng, chứng minh rằng khóa công khai thuộc về người đó. Làm.



ssl

•S SL

SSL (S an toàn secure S socket socket L layer ayer) là một cách để đảm bảo an ninh qua Internet. Nó là một giao thức mã hóa giao tiếp giữa máy chủ web và máy khách nhằm mục đích công cộng Các công nghệ bảo mật như mật mã khóa mở và mật mã khóa chung được sử dụng để chặn dữ liệu và Ngăn chặn giả mạo. Nó được cài đặt theo tiêu chuẩn trong trình duyệt web và dữ liệu có thể được lưu trữ an toàn trên Internet. Nó đã trở thành tiêu chuẩn công nghiệp để trao đổi dữ liệu.

IPSEC
-Psec và nụ cười / MIME

IPsec là một tiêu chuẩn cho giao tiếp được mã hóa trên Internet. Bảo mật được tăng cường bằng cách mã hóa các gói IP để truyền và nhận. Bạn có thể bắt đầu

mạng internet E-mail
S/MIME (S bảo mật an toàn/M đa năng đa năng I mạng internet đau
Tiện ích mở rộng
Tiện ích mở rộng) là một tiêu chuẩn cho mã hóa khóa công khai e-mail và chữ ký số.

thuật ngữ

[Chữ ký số]: Bằng chứng về người gửi dữ liệu và không bị giả mạo công nghệ để kiểm tra xem

[CA]: Tổ chức bên thứ ba chứng nhận tính hợp pháp của khóa công khai

[SSL]: Doanh nghiệp trao đổi dữ liệu trên Internet một cách an toàn. giao thức chuẩn thế giới

kỹ năng

Mã hóa dữ liệu bằng mật mã khóa công khai và chữ ký số, Đảm bảo rằng bạn biết khóa của ai sẽ sử dụng khi giải mã.

試験にチャレンジ

Kỳ thi kỹ sư tin học cơ sở Đặc biệt 2011

Một hệ thống mật mã khóa công khai sử dụng độ khó của việc phân tích thừa số nguyên tố của các số rất lớn là Bất kì.

A: AES B: DSA C: Ý TƯỞNG D: RSA

bình luận

Bẻ khóa mã hóa RSA yêu cầu bao thanh toán số lượng rất lớn có. Đáp án: D

試験にチャレンジ

Kỳ thi kỹ sư công nghệ thông tin cơ bản mùa xuân 2012

Khóa và mã hóa trong mật mã khóa công khai khi gửi, nhận nội dung tài liệu mật Điều nào sau đây là một điều trị thích hợp của các thuật toán?

A: Khóa mã hóa và giải mã được công khai, nhưng thuật toán mã hóa phải được giữ bí mật. phải.

B: Khóa mã hóa được công khai nhưng khóa giải mã và thuật toán mã hóa phải được giữ bí mật. phải.

C: Khóa mã hóa và thuật toán mã hóa được công khai nhưng khóa giải mã phải được giữ bí mật. phải.

D: Khóa giải mã và thuật toán mã hóa được công khai nhưng khóa mã hóa phải được giữ bí mật. phải.

bình luận

Trong mật mã khóa công khai, các khóa mã hóa và thuật toán mã hóa được công khai.

Tuy nhiên, khóa giải mã phải được giữ bí mật. Đáp án: C

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa thu 2014

Anh A có chứng thư số gửi e-mail cho cửa hàng B về sản phẩm.

Khi đặt hàng, anh A ký điện tử bằng khóa riêng của mình và B

Cửa hàng xác minh chữ ký bằng khóa công khai của anh A. Phương pháp này có thể nhận ra

Điều nào sau đây Ở đây, giả sử rằng khóa riêng của anh A chỉ có thể được sử dụng bởi anh A.

Trả lời: Thông tin chi tiết về đơn hàng do anh A gửi cho Shop B không thể tiết lộ cho bên thứ ba.

là.

B: Đơn đặt hàng do ông A gửi có thể được chuyển đến cửa hàng

B. C: Bạn có thể xác nhận rằng đơn đặt hàng đến cửa hàng B là của ông A.

D: Cửa hàng B có thể xác nhận là được ủy quyền bán hàng cho anh A.

bình luận

Điều có thể đạt được bằng cách sử dụng chữ ký điện tử là đơn đặt hàng được thực hiện bởi chính ông A, người gửi. Ngoài ra, đơn đặt hàng của ông A không bị giả mạo

Bạn cũng có thể kiểm tra Đáp án: C

9 an ninh mạng

• Công nghệ an ninh mạng

Khi bạn kết nối máy tính của mình với mạng, bạn có thể kết nối với các máy tính khác qua mạng.
Nó thuận tiện vì nó cho phép bạn truy cập vào máy tính của mình, nhưng ngược lại, có thể truy cập trái phép từ một máy tính khác.
Ngoài ra còn có nguy cơ bị bóc lột. Do đó, có nhiều kỹ thuật khác nhau để ngăn chặn truy cập
trái phép qua mạng.

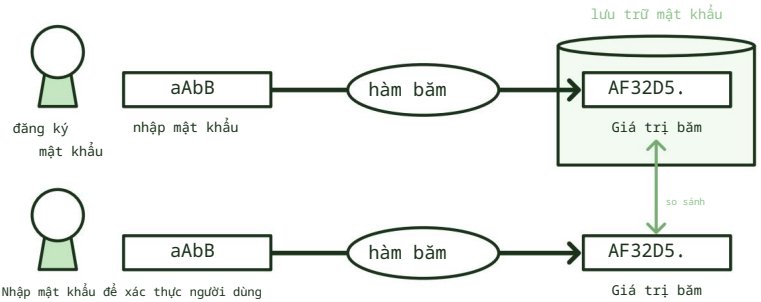
• Xác thực người dùng

ý tưởng
I khi truy cập dữ liệu Nhắc cho D và mật khẩu và nhắc người dùng
Hãy chắc chắn rằng bạn có quyền truy cập. Điều này được gọi là xác thực người dùng. Tuy nhiên, ID và mật khẩu
Nếu mật khẩu của bạn bị đánh cắp, bất kỳ ai khác ngoài bạn đều có thể truy cập được.
Nó là cần thiết để xem xét sự sắp xếp như thay đổi nó theo định kỳ .

• Băm mật khẩu

Khi lưu trữ mật khẩu, hãy chuyển đổi chúng bằng hàm băm thay vì chính mật khẩu
đăng ký giá trị băm. Điều này được gọi là băm. Tương tự để xác thực
Một phương pháp băm mật khẩu đầu vào và so sánh nó với giá trị băm được áp dụng. Mười nghìn
Tuy nhiên, ngay cả khi giá trị băm bị rò rỉ, mật khẩu cũng không thể lấy được, vì vậy
Đây là một phương pháp thường được sử dụng.

<Băm mật khẩu>



Phát hiện giả mạo nội dung bằng cách sử dụng giá trị băm

Giá trị băm được sử dụng để phát hiện sự thay đổi nội dung trên máy chủ web, v.v.
cũng được sử dụng. Băm của từng tệp nội dung trên máy chủ web
lưu trữ giá trị băm và định kỳ tạo giá trị băm từ mỗi tệp.
Liệu nội dung đã bị giả mạo bằng cách tạo và so sánh
Kiểm tra.

•R bán kính ADIUS

RADIUS (Từ xa A xác thực Xác thực Quay số I quay số TRONG n dịch vụ dịch vụ người dùng)

Hệ thống xác thực người dùng truy cập tác phẩm bằng máy chủ xác thực

Giám. Nó được sử dụng cho các kết nối mạng LAN và VPN không dây.

•Xác thực sinh trắc học

Nó không phải là mật khẩu để nhập các chữ cái và số, mà là một vật lý như dấu vân tay của con người hoặc màu mắt.

Xác thực sinh trắc học (biometric authentication) là xác thực dựa trên đặc điểm cá nhân. Ba

Trong xác thực sinh trắc học, ngoài phương pháp trích xuất và xác thực các đặc điểm vật lý, chữ ký

Ngoài ra còn có một phương pháp trích xuất các đặc điểm hành vi từ tốc độ và áp lực viết khi đặt tên và xác thực.

So với ID và mật khẩu, nguy cơ giả mạo ít hơn, độ tin cậy và tiện lợi cao

Tuy nhiên, mặt khác, việc điều chỉnh thiết bị liên quan đến xác suất từ chối sai người và các yếu tố khác.

Phải tính đến cả xác suất ủy quyền sai cho một người.

Nhận dạng

mống mắt Một loại xác thực sinh trắc học, được gọi là mống mắt bên ngoài con ngươi.

Xác thực mống mắt là một phương thức xác thực xác minh danh tính của một người bằng cách sử dụng mẫu hình tròn

Nó được gọi là. Vì mống mắt của người lớn không thay đổi nên thiết bị xác thực
Hầu như không cần cập nhật mẫu.

thuật ngữ

[RADIUS]: Người dùng được sử dụng cho mạng LAN không dây, kết nối VPN, v.v.
hệ thống xác thực

thuật ngữ

[Xác thực sinh trắc học]: Xác thực dựa trên các đặc điểm vật lý như dấu vân tay và mống mắt của con người

Vì vậy, được chứng nhận. Những người xác thực bằng các đặc điểm hành vi như tốc độ viết và áp lực viết

cũng có một công thức

kỹ năng

Trong xác thực sinh trắc học, đặc điểm vật lý và đặc điểm hành vi

Hiểu các phương pháp trích xuất và xác thực cụ thể là gì

Hãy giữ

• Tường lửa

chạy

1. Giữa mạng nội bộ như AN và mạng bên ngoài như Internet

hệ thống tường lửa để ngăn chặn truy cập trái phép vào mạng LAN.

Nó tên Lữ.

Khi tường lửa được cài đặt, giữa mạng nội bộ và mạng bên ngoài,

vùng phi quân sự

Cả hai tạo ra một khu vực bị cô lập. Đây được gọi là DMZ (khu phi quân sự). Ví dụ: khi

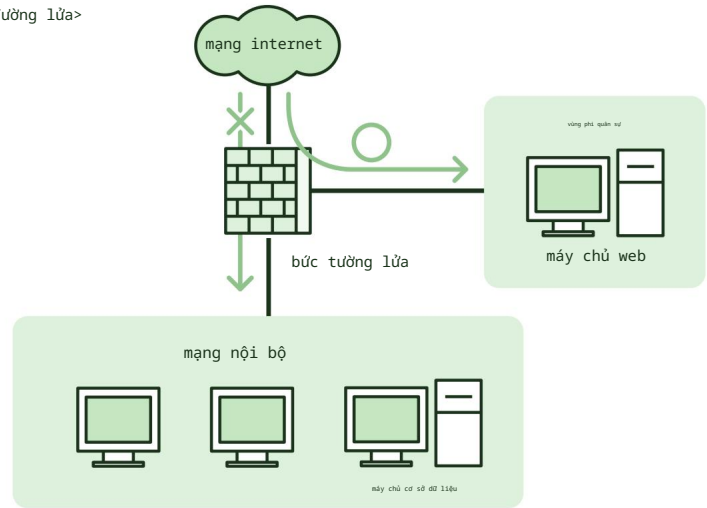
xuất bản một dịch vụ cho người dùng bao gồm máy chủ Web và máy chủ DB lên Internet, thông

thường sẽ thiết lập máy chủ như sau. Chôn cất

Máy chủ web xuất bản thông tin lên Internet nên được đặt trong DMZ và máy chủ DB chứa dữ liệu quan trọng sẽ được cài đặt.

máy chủ trên mạng nội bộ để ngăn chặn truy cập trái phép.

<Tường lửa>



wafu

W.AF

Trái phép bằng cách quản lý tương tác ứng dụng web

Tường lửa có thể ngăn chặn sự xâm nhập là WAF (Web
ứng dụng bức tường lửa
chuyển đến máy tường lửa). Nó kiểm tra nội dung đầu vào được

chủ web và ngăn chặn các cuộc tấn công như SQL injection.

Chặn các yêu cầu truy cập được coi là trái phép.

•Lọc gói tin

Xác định địa chỉ IP đích, địa chỉ IP nguồn và số cổng của gói và

Lọc gói tin là một công nghệ cho phép hoặc chặn việc đi qua các mạng.

Nói. Điều này sẽ lọc ra các gói cố gắng xâm nhập. bộ định tuyến hoặc tập tin

Thực hiện trong tường.

Phán đoán đúng đắn về truyền thông bằng cách sử dụng ARP

ARP là một chương trình tự động lấy địa chỉ MAC từ địa chỉ IP.

Đó là một giao thức. Bằng cách sử dụng cơ chế này, địa chỉ MAC của PC có thể được

địa chỉ và có địa chỉ MAC đã đăng ký trước

Giao tiếp chỉ có thể được phép nếu khách hàng wifi

Nó được sử dụng để xác thực kiến, v.v.

•Ủy quyền

Proxy là một máy tính chuyển tiếp quyền truy cập từ các máy tính trong mạng nội

bộ và thay mặt máy tính đó kết nối với Internet. Proxy truy cập đích kết nối

Bạn có thể ẩn địa chỉ IP của mạng nội bộ vì chỉ lưu lại lịch sử các lần truy cập của bạn.

•Thử nghiệm thâm nhập

hệ thống để khám phá các điểm yếu bảo mật trong máy tính và mạng.

Kiểm thử thâm nhập là kiểm thử thực sự tấn công vào hệ thống đã sửa

Thông qua kiểm tra định kỳ , các lỗ hổng bảo mật mới và cấu hình sai có thể được phát hiện,

bảo mật hệ thống.

Hệ thống phát hiện xâm nhập

ID

Hệ thống phát hiện xâm nhập Còn được gọi là DS (Hệ thống phát hiện xâm nhập), đây là một hệ thống phát hiện và thông báo các hoạt động gian lận trên máy tính và mạng.

Phân tích giao tiếp mạng và phát hiện xem nó có khớp với mẫu phương pháp xâm nhập hay không nếu có sự bất thường.

Thông báo cho quản trị viên khi nó được ban hành.

cửa sau

Để có được quyền truy cập trái phép ngoài lộ trình thông thường, kẻ xâm nhập có thể

Lối vào đằng sau tập hợp được gọi là cửa sau. xâm nhập hoặc tấn công

Vì có khả năng cao là một cửa hậu đã được đặt trong máy chủ nhận được nó,

Bạn cần định dạng đĩa và cài đặt lại hệ điều hành.

thuật ngữ

[Tường lửa]: Bảo vệ mạng nội bộ của bạn khỏi các cuộc tấn công từ bên ngoài

điều

[DMZ]: Vùng giữa mạng bên ngoài và mạng bên trong [Lọc gói]:

Xác định và chuyển địa chỉ IP và số cổng

giới hạn các gói tin

[Proxy]: Kết nối với Internet thay mặt cho mạng nội bộ.

Giấu

[WAF]: Từ các cuộc tấn công từ bên ngoài vào lỗ hổng ứng dụng web

một cái gì đó để bảo vệ

[Thử nghiệm thâm nhập]: Xâm nhập bằng cách thực sự tấn công hệ thống

[Cửa sau] : Một tuyến

đường cửa hậu do kẻ xâm nhập thiết lập để giành quyền truy cập trái phép từ một tuyến đường

khác với tuyến đường bình thường.

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa thu 2014

Mục đích của việc sử dụng WAF (Tường lửa ứng dụng web) là gì?

A: Các cuộc tấn công vào các lỗ hổng do máy chủ web và ứng dụng web gây ra

Cắt.

B: Phát hiện sự xâm nhập của sâu trong máy chủ Web và tự động loại bỏ sâu. C: Ứng dụng

web trong quá trình kiểm tra tích hợp phát triển nội dung máy chủ Web

phát hiện các lỗ hổng và sự không nhất quán trong

D: Phát hiện lỗ hổng bảo mật trong máy chủ web và vá bảo mật hệ điều hành

áp dụng.

bình luận

WAF quản lý các tương tác ứng dụng web để ngăn chặn các cuộc tấn công như SQL

injection và truy cập được coi là trái phép.

yêu cầu dịch vụ. Trả lời: A

試験にチャレンジ

Kỳ thi kỹ sư công nghệ thông tin cơ bản mùa xuân 2015

Xác thực sinh trắc học bao gồm các phương pháp trích xuất và xác thực các đặc điểm vật lý và đặc điểm hành vi.

Có một phương pháp trích xuất và xác thực chữ ký. Điều nào sau đây sử dụng các tính năng hành vi?

A: Xác thực bằng cách trích xuất các tính năng từ góc phân nhánh của các điểm phân nhánh mạch máu và chiều dài giữa các điểm phân nhánh.

là.

B: Xác thực bằng cách trích xuất các đặc trưng từ tốc độ và lực viết khi ký.

C: Xác thực bằng cách trích xuất các đặc điểm của các nếp nhăn hỗn loạn xuất hiện bên ngoài đồng tử

LÀM.

D: Trích xuất các điểm đặc trưng được gọi là chi tiết vụn vặt từ các mẫu được hình thành bởi các đường vân

để xác thực.

bình luận

Tốc độ viết và áp lực viết là những đặc điểm hành vi cá nhân.

trả lời: tôi

試験にチャレンジ

Kỳ thi kỹ sư thông tin cơ bản mùa xuân 2014

Những kẻ tấn công xây dựng gì để xâm nhập vào mạng và máy chủ của công ty?

con muỗi.

A: Đại lý khách hàng mỏng

B: Định tuyến nghiêm ngặt

C: Pháp y kỹ thuật số

D: Cửa sau

bình luận

Những kẻ tấn công thiết lập các cửa hậu để truy cập trái phép bên ngoài các kênh thông thường. sẽ được bao gồm.

Đáp án: D