Câu hỏi LO4 tham khảo:

1. Khóa phiên (Session key) là gì? Khóa phiên có ưu điểm gì so với khóa bí mật chia sẻ (secret shared key)? Trình bày và giải thích một giao thức phát sinh khóa phiên mà bạn biết.

a. Khóa phiên (session key):

• Được phát sinh bằng một thuật toán phát sinh khóa phiên

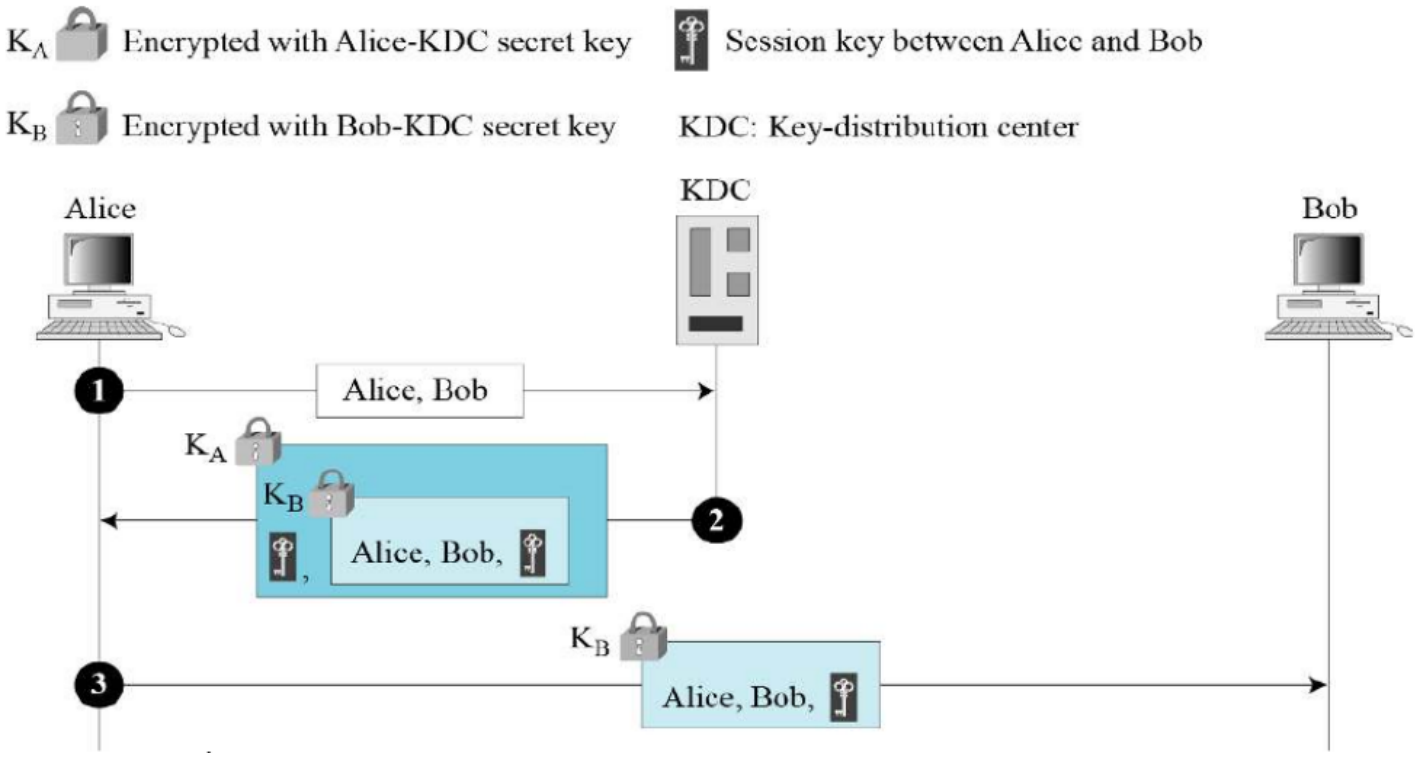
• Chỉ có tác dụng xác thực tại một phiên làm việc hiện tại, hết phiên làm việc thì khóa đó sẽ không còn có tácdụng

• Khóa phiên này có thể đóng vai trò như là khóa bí mậtchia sẻ trong hệ thống mã hóa khóa bí mật, dùng khóa phiên sẽ hạn chế được tấn công nghe lén khóa

b. Ưu điểm khóa phiên so với khóa bí mật chia sẻ (secret shared key):

- Bảo mật tương đối: Khóa phiên được tạo ra trong quá trình trao đổi dữ liệu giữa các bên tham gia phiên. Vì vậy, nó tồn tại trong một thời gian ngắn hơn so với khóa bí mật chia sẻ, làm giảm khả năng bị tấn công và phá vỡ khóa. Khi phiên kết thúc, khóa phiên cũng được hủy bỏ.
- Hiệu suất: Sử dụng khóa phiên, các bên có thể sử dụng thuật toán mã hóa và giải mã hiệu quả hơn. Khóa phiên thường được tạo ra từ một thuật toán mã hóa đối xứng, như AES (Advanced Encryption Standard), mà có hiệu suất cao hơn so với thuật toán mã hóa không đối xứng như RSA.
- Quản lý khóa đơn giản hơn: Với khóa phiên, không cần phải quản lý một số lượng lớn các khóa bí mật chia sẻ giữa các bên. Thay vào đó, mỗi phiên có một khóa phiên duy nhất được tạo ra động, giảm độ phức tạp của việc quản lý khóa.
- Khả năng đảm bảo tính riêng tư: Vì khóa phiên tồn tại trong thời gian ngắn và không được chia sẻ giữa các phiên khác nhau, nó đảm bảo tính riêng tư cao hơn. Ngược lại, khóa bí mật chia sẻ phải được chia sẻ giữa các bên và tồn tại trong thời gian dài, tăng nguy cơ bị rò rỉ hoặc lộ thông tin.

c. Trình bày và giải thích một giao thức phát sinh khóa phiên mà bạn biết.

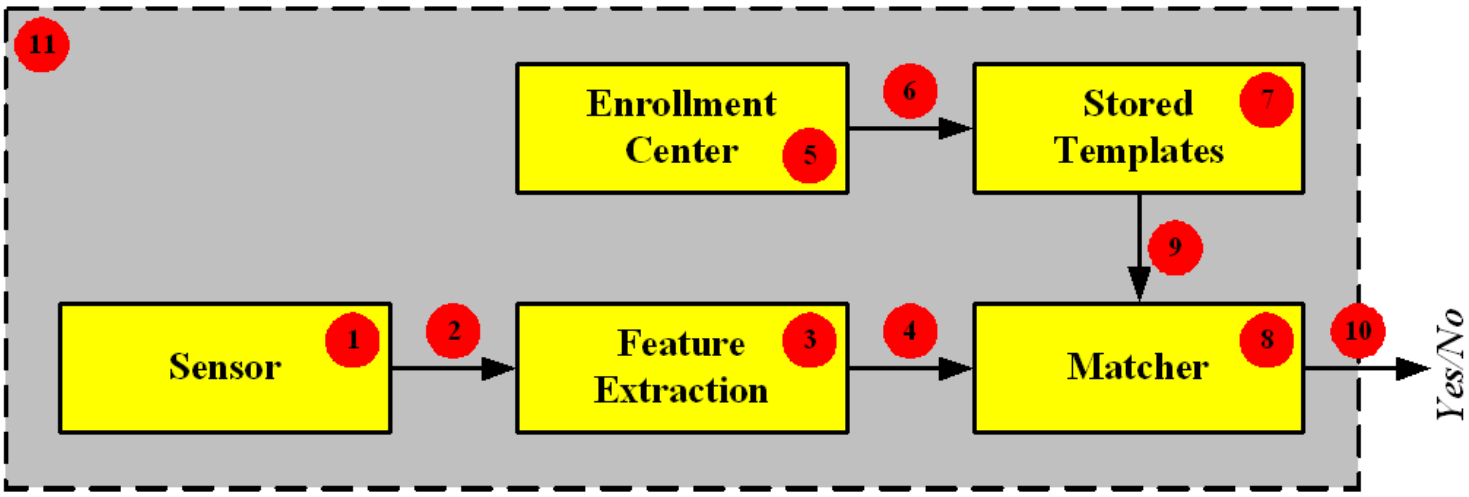


- Giải thích :

2. Chứng thực thực thể bằng sinh trắc học (biometrics) là gì? Trình bày các thành phần cơ bản cần có trong một hệ thống chứng thực sinh trắc học (ví dụ vân tay). Nêu ưu điểm và nhược điểm của phương pháp này. Ở Việt Nam, phương pháp chứng thực sinh trắc học hiện nay được áp dụng ở những lĩnh vực nào?

a. Chứng thực thực thể bằng sinh trắc học (biometrics)

- Sinh trắc học (Biometric) là phép đo lường về các đặc tính sinh lý học hoặc hành vi học mà nhận dạng một con người.
- Sinh trắc học đo lường các đặc tính mà không thể đoán, ăn cắp hoặc chia sẻ.
- Chứng thực thực thể bằng sinh trắc học là việc sử dụng các đặc điểm vật lý hoặc hành vi duy nhất của một người để xác nhận danh tính của họ. Các đặc điểm này bao gồm vân tay, khuôn mặt, giọng nói, mống mắt, vân mạch máu, và nhiều hơn nữa dùng để xác định và chứng thực danh tính của họ.



Giải thích:

Components (thành phần)

▪ Enrollment (ghi nhận vào)

Trước khi dùng bất cứ kỹ thuật sinh trắc học để chứng thực, đặc tính tương ứng của mỗi người trong cộng động cần phải có sẵn trong CSDL, quá trình này được gọi là enrollment

▪ Authentication (chứng thực):

- Chứng thực (Authentcation) được thực hiện bởi sự thẩm tra (Verification) hoặc nhận dạng (identication)

+ Verification: Đặc tính của một người được so khớp với một mẫu tin đơn trong CSDL để xác định cô ta có phải là người mà cô ta đang tự khai không

+ Identication: Đặc tính của một người được so khớp với tất cả các mẫu tin có trong CSDL để xác định cô ta có một mẫu tn trong CSDL.

▪ Techniques (Kỹ thuật):

Các kỹ thuật sinh trắc học có thể được chia thành hai hướng chính: sinh lý học và dáng điệu học:

- Sinh lý học: Kỹ thuật sinh lý học dựa trên những đặc điểm sinh lý tự nhiên của cơ thể con người. Ví dụ về kỹ thuật sinh lý học bao gồm:

+ Nhận dạng dấu vân tay: Dấu vân tay được sử dụng như một biểu diễn độc nhất của mỗi người. Kỹ thuật này dựa trên việc sử dụng các đặc trưng của dấu vân tay, chẳng hạn như hình dạng, đường viền, hoặc điểm đặc biệt, để xác định danh tính.

+ Nhận dạng khuôn mặt: Kỹ thuật này sử dụng các đặc trưng của khuôn mặt, chẳng hạn như hình dạng của mắt, mũi, miệng, hoặc bàn chải da mặt, để xác định danh tính. Các phương pháp như phân tích hình dạng khuôn mặt, phân tích các điểm đặc biệt trên khuôn mặt, hoặc sử dụng mạng nơ-ron học sâu (deep neural networks) có thể được áp dụng.

+ Nhận dạng dấu mống mắt: Kỹ thuật sử dụng dấu mống mắt để xác định danh tính. Mỗi người có một dấu mống mắt duy nhất, được tạo thành từ các đặc trưng như hình dạng và kích thước của mống mắt, các mạng mạch màu sắc, và các đường viền.

- Dáng điệu học: Kỹ thuật dáng điệu học tập trung vào việc phân tích và nhận dạng các đặc điểm về cử chỉ và chuyển động của con người. Ví dụ về kỹ thuật dáng điệu học bao gồm:
+Nhận dạng chữ ký động: Kỹ thuật này dựa trên việc phân tích các đặc trưng của chữ ký khi viết, chẳng hạn như nét viết, áp lực, độ nghiêng và tốc độ. Các thuật toán máy học và phân tích hình ảnh có thể được sử dụng để xác định chữ ký của một người cụ thể.
+ Nhận dạng giọng nói: Kỹ thuật này sử dụng các đặc trưng của giọng nói, chẳng hạn như tần số, âm giai, cường độ và nhịp điệu, để xác định danh tính. Các thuật toán xử lý tín hiệu âm thanh hoặc mô hình học sâu có thể được áp dụng để phân tích và nhận dạng giọng nói.
+Nhận dạng vận tốc gõ phím: Kỹ thuật này dựa trên việc phân tích các đặc trưng của quá trình gõ phím, chẳng hạn như thời gian giữ phím, khoảng cách giữa các phím và tốc độ gõ. Các thuật toán máy học và phân tích dữ liệu có thể được áp dụng để xác định danh tính dựa trừng vận tốc gõ phím.

▪ Accuracy (độ chính xác)
Độ chính xác (Accuracy) của các kỹ thuật sinh trắc học được đo lườngbằng cách dùng hai tham số:
+False Rejection Rate (FRR):là tỷ lệ các trường hợp mà hệ thống sinh trắc học từ chối nhận dạng một cá nhân chính xác. Nó đo lường khả năng của hệ thống từ chối sai, tức là từ chối chấp nhận một người hợp lệ. FRR được tính bằng cách chia số lần từ chối sai cho tổng số lần có thể nhận dạng đúng của một cá nhân.
+ False Acceptance Rate (FAR): FAR là tỷ lệ các trường hợp mà hệ thống sinh trắc học chấp nhận một cá nhân không chính xác. Nó đo lường khả năng của hệ thống chấp nhận sai, tức là chấp nhận một người không hợp lệ. FAR được tính bằng cách chia số lần chấp nhận sai cho tổng số lần có thể chấp nhận sai của hệ thống.
▪ Applications (các cứng dụng):
- Rất nhiều ứng dụng của sinh trắc học đã được áp dụng trong nhiều lĩnh vực khác nhau.
+ Kiểm soát truy cập nơi làm việc
+ Điều khiển truy xuất hệ thống và thông tin nhạy cảm
+ Thực thi các giao dịch thương mại điện tử trực tuyến
+ Nhận dạng tội phạm bằng cách phân tích DNA
+ Kiểm soát nhập cư
- Ví dụ: truy xuất các thiết bị, các hệ thống thông tin, giao dịch ở các điểmbán (trả tiền) điều tra bằng cách phân tích AND hoặc vân tay,..
b. Nêu ưu điểm và nhược điểm của phương pháp này.
- Ưu điểm
▪ Có thể rất chính xác
▪ Nhanh: thời gian chứng thực nhỏ hơn 1s
▪ Sự tác động của người dùng thấp
▪ Kết hợp nhiều yếu tố: vân tay, võng mạc, giọng nói,…
▪ Biometrics không thể bị mất, đánh cấp, bỏ quên. Nó nhất quán và vĩnh cửu
▪ Nó không thể được chia sẻ hoặc dùng bởi người khác
▪ Không đòi hỏi phải ghi nhớ như mật khẩu, mã Pin
▪ Biometric luôn luôn sẳn dùng cho cá nhân và duy nhất

- Nhược điểm
▪ Giá thành: triển khai hệ thống sinh trắc học đòi hỏi chi phí cho phần cứng và phần mềm.
▪ Có thể nhận diện sai: mặc dù đúng người nhưng hệ thống không chấp nhận
▪ Các bộ đọc luôn đặc tính của sinh trắc học có những lỗi nhất định
    • Từ chối người dùng hợp lệ
    • Chấp nhận người dùng không hợp lệ

c. Ở Việt Nam, phương pháp chứng thực sinh trắc học hiện nay được áp dụng ở những lĩnh vực nào?

- An ninh và quản lý biên giới: Các phương pháp sinh trắc học như nhận dạng khuôn mặt, nhận dạng dấu vân tay và nhận dạng giọng nói được sử dụng để xác định danh tính và kiểm soát truy cập trong các cơ sở quản lý biên giới, sân bay, và các khu vực an ninh quan trọng khác.VD:ại các cửa khẩu quốc tế ở Việt Nam, hệ thống nhận dạng khuôn mặt được sử dụng để xác định danh tính của người đi qua. Khi một người tiến cận cửa khẩu, hệ thống sẽ quét và so sánh khuôn mặt của người đó với cơ sở dữ liệu để xác định xem họ có phải là người hợp lệ hay không.
- Quản lý nhân sự và chấm công: Các công ty và tổ chức sử dụng công nghệ sinh trắc học để xác thực nhân viên và quản lý chấm công. Ví dụ, nhận dạng khuôn mặt có thể được sử dụng để kiểm tra danh tính của nhân viên khi vào và ra khỏi công ty.
- Giao dịch tài chính và ngân hàng: Sinh trắc học được áp dụng trong các hệ thống xác thực giao dịch tài chính và ngân hàng nhằm đảm bảo an toàn và bảo mật thông tin cá nhân của khách hàng. Ví dụ, nhận dạng dấu vân tay, nhận dạng khuôn mặt và xác thực giọng nói có thể được sử dụng trong quá trình xác thực khách hàng.
- Quản lý sự y tế: Công nghệ sinh trắc học có thể được áp dụng trong quản lý và xác thực thông tin y tế của bệnh nhân, đảm bảo quyền riêng tư và bảo mật dữ liệu y tế quan trọng.Một số bệnh viện và cơ sở y tế lớn ở Việt Nam áp dụng công nghệ sinh trắc học để xác thực danh tính và quản lý thông tin bệnh nhân. Ví dụ, hệ thống nhận dạng khuôn mặt có thể được sử dụng để xác nhận danh tính của bệnh nhân khi họ đến khám hoặc truy cập dữ liệu y tế của mình.
- Truy cập vào thiết bị di động: Một số thiết bị di động sử dụng các phương pháp như nhận dạng khuôn mặt hoặc quét dấu vân tay để xác thực người dùng và bảo vệ dữ liệu cá nhân.Nhiều điện thoại di động hiện nay đã tích hợp công nghệ nhận dạng khuôn mặt hoặc quét dấu vân tay để xác thực người dùng và mở khóa thiết bị. Ví dụ, một người dùng có thể sử dụng tính năng nhận dạng khuôn mặt trên điện thoại để mở khóa và truy cập vào các ứng dụng và dữ liệu cá nhân của mình.

3. **Điều khiển truy cập là gì? Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.**

a. Điều khiển truy cập
- Cấp phép hoặc từ chối phê duyệt sử dụng các tài nguyên xác định.
- Là cơ chế của hệ thống thông tin cho phép hoặc hạn chế truy cập đến dữ liệu hoặc các thiết bị.
- Nhiệm vụ điều khiển truy cập trong an ninh máy tính bao gồm:
▪ Nhận diện: Người dùng trình ra các vật chứng để chứng minh sự nhận viện
▪ Chứng thực: Kiểm tra, xác minh các ủy quyến
▪ Ủy quyền: Cấp các quyền để thực hiện hành động truy cập
▪ Truy cập: thực hiện truy xuất các tài nguyên xác định

b. Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.

- Mật khẩu (Password):một chuỗi ký tự hoặc một nhóm từ được sử dụng để xác thực thực thể

- Chứng thực mật khẩu là phương pháp đơn giản và lâu đời nhất, được gọi là Password-based Authentication, password là một thứ mà claimant biết.
- Một Password được dùng khi một người dùng cần truy xuất một hệ thống để sử dụng nguồn tài nguyên của hệ thống.
- Mỗi người dùng có một định danh người dùng (user identification) công khai và một password bí mật.
- Có 2 cơ chế password:
  - Fixed password
  - và one-time password

- Sinh trắc học (Biometrics):

4. **Mật khẩu (password) là gì? Mật khẩu cố định (fixed password) và mật khẩu dùng một lần (one time password) khác nhau như thế nào? Trình bày điểm mạnh và điểm yếu của 2 loại mật khẩu.**

a. Mật khẩu (password)

Mật khẩu: một chuỗi ký tự hoặc một nhóm từ được sử dụng đề xác thực thực thế

- Chứng thực mật khẩu là phương pháp đơn giản và lâu đời nhất, được gọi là Password-based Authentication, password là một thứ mà claimant biết.
- Một Password được dùng khi một người dùng cần truy xuất một hệ thống để sử dụng nguồn tài nguyên của hệ thống.
- Mỗi người dùng có một định danh người dùng (user identification) công khai và một password bí mật.
- Có 2 cơ chế password:
  - Fixed password
  - One-time password

Fixed password	One-time password
Dùng được nhiều lần và có thê thay đổi được. Ví dụ: Password sv đăng nhập vào trang sv.iuh.edu	Chỉ dùng được 1 lần. Vì dụ: OTP
- Bảo mật thấp hơn	- Bảo mật cao hơn, nếu có bị đánh cắp hay rò ri thì sẽ kg sử dụng được
Có thể dễ dàng đặt mật khẩu yếu hoặc sử dụng mật khẩu trùng lặp	- Mật khẩu được tạo ngẫu nhiên và có độ dài lớn, khó đoán trước
Đòi hỏi người dùng phải nhớ và quản lý nhiều mật khẩu	-Mật khẩu được tạo và cung cấp bởi hệ thống, không cần nhớ
Dễ sử dụng và tiện lợi cho người dùng	Cần sự hỗ trợ của hệ thống để tạo và cung cấp mật khẩu
Thường được sử dụng trong các hệ thống truy cập dài hạn	Thường được sử dụng trong các giao dịch ngắn hạn, tạm thời
Cần sử dụng các biện pháp bảo mật bổ sung như xác thực hai yếu tố	Mật khẩu sử dụng một lần giúp tăng cường bảo mật
Phù hợp cho các hệ thống yêu cầu sự tiện lợi và quản lý đơn giản	Phù hợp cho các giao dịch tài chính, truy cập tạm thời

b. Trình bày điểm mạnh và điểm yếu của 2 loại mật khẩu

Điểm mạnh	1. Tiện lợi và dễ sử dụng cho người dùng.	1. Mật khẩu chỉ sử dụng một lần, tăng cường bảo mật.
	2. Dễ nhớ và tiện dụng cho đăng nhập thường xuyên.	2. Khả năng chống lại các cuộc tấn công đoán mật khẩu.
	3. Đơn giản và không yêu cầu sự hỗ trợ từ hệ thống.	3. Giảm khả năng bị đánh cắp mật khẩu.

Điểm yếu	1. Dễ bị đoán và xâm phạm bởi tin tặc nếu mật khẩu yếu.	1. Cần sự hỗ trợ từ hệ thống để tạo và cung cấp mã OTP.
	2. Khả năng bị tấn công bằng các phương pháp tấn công mạng.	2. Đòi hỏi sự kết nối mạng hoặc điện thoại di động.
	3. Nguy cơ bị đánh cắp mật khẩu nếu sử dụng trên nhiều tài khoản.	3. Khả năng mất mã OTP nếu không có quy trình xử lý phù hợp.

5. **Trình bày các loại mã OTP, nêu ưu điểm và nhược điểm của từng loại. Đưa ra một hệ thống mà bạn biết có sử dụng mật khẩu dùng một lần (one time password) và mô tả tình huống mà bạn có sử dụng mật khẩu để chứng thực người dùng/giao dịch. Nêu mục tiêu của việc chứng thực này.**

a. Trình bày các loại mã OTP, nêu ưu điểm và nhược điểm của từng loại.

- Mã OTP được tạo ra dựa trên bộ vi xử lý hoặc thẻ khóa kích thước bỏ túi tạo mã số và chữ số để xác thực quyền truy cập vào hệ thống hoặc giao dịch. Sau 30s đến 2 phút, mã này lại bị thay đổi một lần.
- Mã OTP có thể được triển khai bằng phần cứng, phần mềm hoặc theo yêu cầu.
- Mã OTP được dùng làm bảo mật 2 lớp trong các giao dịch xác minh đăng nhập và đặc biệt là giao dịch với tài khoản ngân hàng, nhờ đó, giảm thiểu tối đa rủi ro bị tấn công khi lộ mật khẩu hay tin tặc tấn công.

• Những loại mã OTP phổ biến hiện nay

- SMS OTP:
  + Mã OTP được gửi qua SMS đến số điện thoại của khách hàng khi cần xác thực giao dịch
  +Đa số ngân hàng tại Việt Nam: OTP vietcombank, otp techcombank, otp sacombank, otp bidv
  + Bạn đang ở trong khu vực sóng kém hoặc ngoài vòng phủ sóng thì bạn không thể nhận được mã SMS OTP→ SMS OTP sẽ không sử dụng được.
- TOKEN KEY (TOKEN CARD):
  + Là thiết bị bảo mật mà doanh nghiệpcung cấp dịch vụ cung cấp cho khách hàng
  + Token Key có thể tạo ra mã OTP gồm 6 ký tự, cứ sau mỗi phút nó sẽ tự động được tạo ra mà không cần thông qua Internet.
  + Mỗi tài khoản phải đăng ký riêng một Tokey key, và thông tin về Token key được thay đổi sau một khoản thời gian quy định.
  + Loại thiết bị này cực kỳ tiện lợi khi luôn mang theo bên người. Tuy nhiên, bạn cần phải bảo quản thật cẩn thận.
- SMART OTP – SMART TOKEN:
  + Smart OTP là dạng OTP tốt nhất hiện nay
  + Smart OTP là sự kết hợp hài hoà giữa Token Key và SMS OTP.
  + Smart OTP có thể được sử dụng mọi lúc mọi nơi vì nó được tích hợp sẵn trên ứng dụng của điện thoại. Khi có phiên giao dịch trực tuyến thì Smart OTP sẽ được gửi về ứng dụng trên smartphone.
  + Hai ngân hàng đã sử dụng cách thanh toán tiền Online bằng phương thức Smart OTP và SMS OTP là Vietcombank và TPBank. Người dùng phải kê khai thông tin và đăng ký trực tiếp với ngân hàng họ muốn. Lưu ý, mỗi thiết bị chỉ nên dùng 1 mã OTP riêng biệt.

6. Chữ ký số (digital signitures) là gì? Mục tiêu của chữ ký số? Trình bày hiện trạng áp dụng chữ ký số ở Việt Nam

a. Chữ ký số (digital signitures)

• Khái niệm về Digital Signature được để xuất bởi Diffie &Hellman (1976).

• 1989, phiên bản thương mại Chữ ký số đầu tiên trong Lotus Notes, dựa trên RSA

• Chữ ký số là một dạng của chữ ký điện tử. Chữ ký số là thông tin đi kèm theo các tài liệu điện tử như Word, Excel, PDF,…; hình ảnh; video…) nhằm đảm bảo tính xác thực của người ký. Nó mã hóa tài liệu và nhúng vĩnh viễn thông tin vào đó. Bất kỳ thay đổi nào trong các tài liệu sau khi nó đã được ký là vô hiệu, do đó nó bảo vệ, chống lại sự giả mạo chữ ký và thông tin giả mạo. Chữ ký số đảm bảo về mặt pháp lý
• Chữ ký số giúp các tổ chức duy trì ký xác thực, trách nhiệm giải trình, tính toàn vẹn dữ liệu và không thoái thác tài liệu điện tử và các hình thức ký kết.

b. Mục tiêu của chữ ký số

Mục tiêu an toàn
• Xác thực (Authentication)
• Chống khai thác

c. Hiện trạng áp dụng chữ ký số ở Việt Nam

Hiện trạng áp dụng chữ ký số ở Việt Nam đã có sự phát triển và áp dụng rộng rãi trong nhiều lĩnh vực. Dưới đây là một tóm tắt về hiện trạng áp dụng chữ ký số ở Việt Nam:

1. Luật và quy định:
   - Việt Nam đã ban hành nhiều luật và quy định liên quan đến chữ ký số, bao gồm Luật Chữ ký số (năm 2005), Nghị định về Chữ ký số (năm 2018), và các hướng dẫn chi tiết khác.
   - Các quy định này cung cấp khung pháp lý và hướng dẫn về việc sử dụng, công nhận và bảo vệ chữ ký số tại Việt Nam.
2. Ứng dụng:
   - Chữ ký số được sử dụng rộng rãi trong nhiều lĩnh vực, bao gồm:
     - Giao dịch điện tử: Chữ ký số được sử dụng trong giao dịch trực tuyến, chẳng hạn như mua bán hàng hóa, chuyển nhượng tài sản, thanh toán điện tử, v.v.
     - Văn bản điện tử: Chữ ký số được sử dụng để xác thực tính toàn vẹn và nguồn gốc của văn bản điện tử, chẳng hạn như hợp đồng, biên bản, văn bản quy phạm pháp luật, v.v.
     - Dịch vụ công trực tuyến: Chữ ký số được sử dụng trong các dịch vụ công trực tuyến như khai thuế điện tử, đăng ký kinh doanh, xác nhận hồ sơ, v.v.
3. Cơ quan chứng thực:
   - Cơ quan chứng thực chữ ký số chính tại Việt Nam là Trung tâm Chứng thực Chữ ký số (VinaCa), thuộc Trung tâm Tin học và Thống kê Tổng cục Thuế.
   - VinaCa có nhiệm vụ chứng thực và quản lý chữ ký số, cung cấp chứng chỉ số và dịch vụ liên quan cho các tổ chức và cá nhân.
4. Chuyển đổi số và chữ ký số:
   - Chữ ký số đóng vai trò quan trọng trong quá trình chuyển đổi số của Việt Nam, giúp thúc đẩy sự phát triển của kinh tế số và giao dịch điện tử.
   - Chữ ký số cũng góp phần tăng cường tính bảo mật và xác thực trong việc sử dụng các dịch vụ trực tuyến và văn bản điện tử.

7. **Gợi ý: Khái niệm chữ ký số: ứng dụng của mã hóa khóa công khai, người dùng có (KUA, KRA); Tạo chữ ký: SAM = E(KRA, M) hoặc SAM=E(KRA, H(M)) – giải thích; Thẩm tra chữ ký D(KUA, SAM) → Yes/No – Giải thích; Mục tiêu của chữ ký số; Hiện trạng áp dụng chữ ký: 4 lĩnh vực đó là cơ quan Thuế, Bảo hiểm xã hội, Hải quan và Chứng khoán.**

Dưới đây là ví dụ cụ thể về hiện trạng áp dụng chữ ký số trong bốn lĩnh vực: cơ quan Thuế, Bảo hiểm xã hội, Hải quan và Chứng khoán:

1. Cơ quan Thuế:
   - Áp dụng chữ ký số trong việc khai thuế điện tử, gửi hồ sơ thuế và các giao dịch liên quan.
   - Ví dụ: Doanh nghiệp sử dụng chữ ký số để ký và gửi báo cáo thuế hàng tháng, khai thuế GTGT (giá trị gia tăng), hoặc xác nhận hồ sơ liên quan đến thuế.

2. Bảo hiểm xã hội:
- Sử dụng chữ ký số trong các quy trình liên quan đến bảo hiểm xã hội, bao gồm đăng ký, nộp hồ sơ, yêu cầu thanh toán và xác nhận thông tin.
- Ví dụ: Nhà tuyển dụng sử dụng chữ ký số để ký và gửi các báo cáo bảo hiểm xã hội hàng tháng, đề nghị thanh toán bồi thường cho nhân viên, hoặc xác nhận thông tin về bảo hiểm xã hội.

3. Hải quan:
- Sử dụng chữ ký số trong quá trình khai báo hải quan và các giao dịch với cơ quan Hải quan.
- Ví dụ: Doanh nghiệp sử dụng chữ ký số để ký và gửi hồ sơ khai báo hàng hóa, yêu cầu giải quyết thủ tục hải quan, hoặc xác nhận thông tin về giao dịch xuất nhập khẩu.

4. Chứng khoán:
- Áp dụng chữ ký số trong quá trình giao dịch chứng khoán trực tuyến, xác nhận và xử lý các yêu cầu từ nhà đầu tư.
- Ví dụ: Nhà đầu tư sử dụng chữ ký số để xác thực và ký các lệnh mua bán chứng khoán trực tuyến, xác nhận giao dịch và yêu cầu các dịch vụ liên quan đến tài khoản chứng khoán.

8. Mô tả chứng thư số là gì? Mục tiêu của chứng thư số? Nội dung có trong chứng thư số là gồm những nội dung gì?

a. Mô tả chứng thư số

- Là một văn bản cung cấp khóa công khai
- được cung cấp bởi một tổ chức gọi là tổ chức cung cấp dịch vụ chứng thư số (certificate authority, hay viết tắt là CA).
- Chứng thư số hoạt động nhờ vào nguyên lý bên thứ ba tin cậy (trusted third party – TTP), ở đây bên thứ ba chính là CA. Thông thường, 2 bên giao tiếp với nhau không tin nhau, tuy nhiên, nếu họ cùng tin vào một bên thứ ba (TTP), và bên thứ ba đã xác thực 2 bên này, thì 2 bên này sẽ tin tưởng lẫn nhau
- "Chứng thư số" là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cơ quan, tổ chức, cá nhân,từ đó xác nhận cơ quan, tổ chức, cá nhân là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng (theo Khoản 7, Điều 3, Nghị định 130/2018/NĐ-CP)

b. Mục tiêu của chứng thư số

- Xác thực
-Chống khai thác
- Đảm bảo tính bí mật, tòa vẹn

c. Nội dung có trong chứng thư số là gồm những nội dung gì?

Nội dung của chứng thư số theo chuẩn X.509

Tiêu chuẩn về *Chứng thư số* dựa trên cơ sở hạ tầng *khóa công khai* phổ biến nhất hiện này là X.509 được ban hành bởi ITU-T (International Telegraph Union - Telecom, Tổ chức viễn thông quốc tế (về lĩnh vực viễn thông), thuộc Liên hợp quốc).

Những nội dung thông tin cơ bản theo chuẩn X.509

Version: Chỉ định phiên bản của chứng nhận X.509.

Serial Number: Số loạt phát hành được gán bởi CA. Mỗi CA nên gán một mã số loạt duy nhất cho mỗi giấy chứng nhận mà nó phát hành.

Signature Algorithm: Thuật toán chữ ký chỉ rõ thuật toán mã hóa được CA sử dụng để ký giấy chứng nhận. Trong chứng nhận X.509 thường là sự kết hợp giữa thuật toán băm (chẳng hạn như MD5) và thuật toán khóa công cộng (chẳng hạn như RSA).

Issuer Name: Tên tổ chức CA phát hành chứng thực.(Theo chuẩn X.500 thì gọi là Tên phân biệt - X.500 Distinguised Name, X.500 DN). Hai CA khác nhau không được sử dụng cùng một tên phát hành.

Validity Period: gồm hai giá trị chỉ định khoảng thời gian mà giấy chứng nhận có hiệu lực: not-before và not-after.

Not-before: thời gian chứng nhận bắt đầu có hiệu lực;

Not-after: thời gian chứng nhận hết hiệu lực.

Các giá trị thời gian này được đo theo chuẩn thời gian Quốc tế, chính xác đến từng giây.

Subject Name: Tên chủ thể được cấp chứng thực.

Public Key: Chìa khoá công khai của chủ thể được cấp chứng thực.

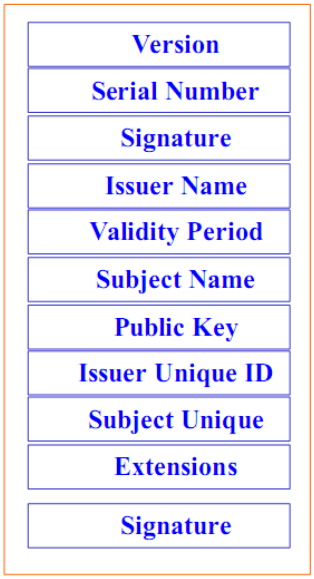
Issuer Unique ID&Subject Unique ID: Được đưa vào sử dụng từ X.509 phiên bản 2, dùng để xác định hai tổ chức CA hoặc hai chủ thể khi chúng có cùng DN. RFC 2459 đề nghị không nên sử dụng hai trường này.

Extensions: Chứa các thông tin bổ sung cần thiết mà người thao tác CA muốn đặt vào chứng nhận. (Mới được đưa ra trong X.509 phiên bản 3).

Signature: chữ ký số được tổ chức CA áp dụng.

Tổ chức CA tạo chữ ký bằng khóa bí mật với kiểu thuật toán mã được quy định trong trường thuật toán chữ ký.

Chữ ký bao gồm tất cả các phần khác trong giấy chứng nhận. (Qua đó thể hiện CA chứng nhận cho tất cả các thông tin khác trong giấy chứng thực, chứ không chỉ cho tên chủ thể và khóa công khai).



9. Hệ thống quản lý an toàn thông tin (ISMS) là gì? Mục tiêu của hệ thống an toàn toàn thông tin?

a. Hệ thống quản lý an toàn thông tin (ISMS) :

- Hệ thống quản lý an toàn thông tin (Information Security Management System - ISMS) là công cụ để các nhà lãnh đạo quản lý thực hiện việc giám sát, quản lý hệ thống thông tin, tăng cường mức độ an toàn, bảo mật, giảm thiểu rủi ro cho hệ thống thông tin, đáp ứng được mục tiêu của doanh nghiệp, tổ chức.
- Hệ thống quản lý an toàn thông tin là một hệ thống đưa ra các phương pháp đánh giá việc theo dõi; bảo vệ và quản lý hệ thống thông tin, dữ liệu. Việc mất thông tin trong bất cứ trường hợp nào; dù ít hay nhiều cũng gây ra thiệt hại cho tổ chức. Thậm chí có thể khiến tổ chức sụp đổ.
- Thiết kế và triển khai Hệ thống ISMS phụ thuộc vào mục tiêu, các yêu cầu về ATTT cần phải đạt được, các quy trình đang vận hành, quy mô và cơ cấu của tổ chức...
- Hệ thống ISMS cũng đòi hỏi phải luôn được xem xét, cập nhật để phù hợp với những thay đổi của tổ chức và nâng cao mức độ an toàn với Hệ thống lưu trữ, xử lý thông tin.
- Tổ chức cũng cần cân nhắc chi phí đầu tư xây dựng và triển khai ISMS phù hợp với nhu cầu đảm bảo ATTT.
- Sau khi xây dựng hệ thống ISMS thì doanh nghiệp sẽ nhận được Chứng chỉ An toàn bảo mật thông tin

b. Mục tiêu của hệ thống an toàn toàn thông tin

- Việc áp dụng ISMS là quyết đinh mang tính chiến lược của một tổ chức.

Hệ thống quản lý an toàn thông tin (ISMS) duy trì tinh bảo mãt, tinh toàn vẹn và tỉnh sắn sảng của thông tin bằng cách áp dung một quá trình quản lý rủi ro và mang lai sư tin cây cho các bên quan tâm răng các rùi ro đã được quản lý đây đù.

-Đảm bảo ATTT của tổ chức, đối tác và khách hàng, giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.

- Giúp nhân viên tuân thủ việc đảm bảo ATTT trong hoat động nghiệp vụ thường ngày, Các sư cô ATTT do người dùng gây ra sẽ được han chế tôi đa khi nhân viên được đào tạo, nâng cao nhân thức ATTT.|

- Giúp hoạt đông đảm bảo ATTT luôn được duy tri và cải tiến. Các biên pháp kỳ thuất và chinh sách tuân thủ được xem xét, đánh giá, đo lường hiệu quả và cập nhật định kỳ.

- Đảm bảo hoạt đông nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cổ liên quan đến ATTT

10. Trình bày các đặc điểm của hàm băm? Trình bày giải pháp xử lý mật khẩu trước khi lưu vào cơ sở dữ liệu và giải thích vì sao?

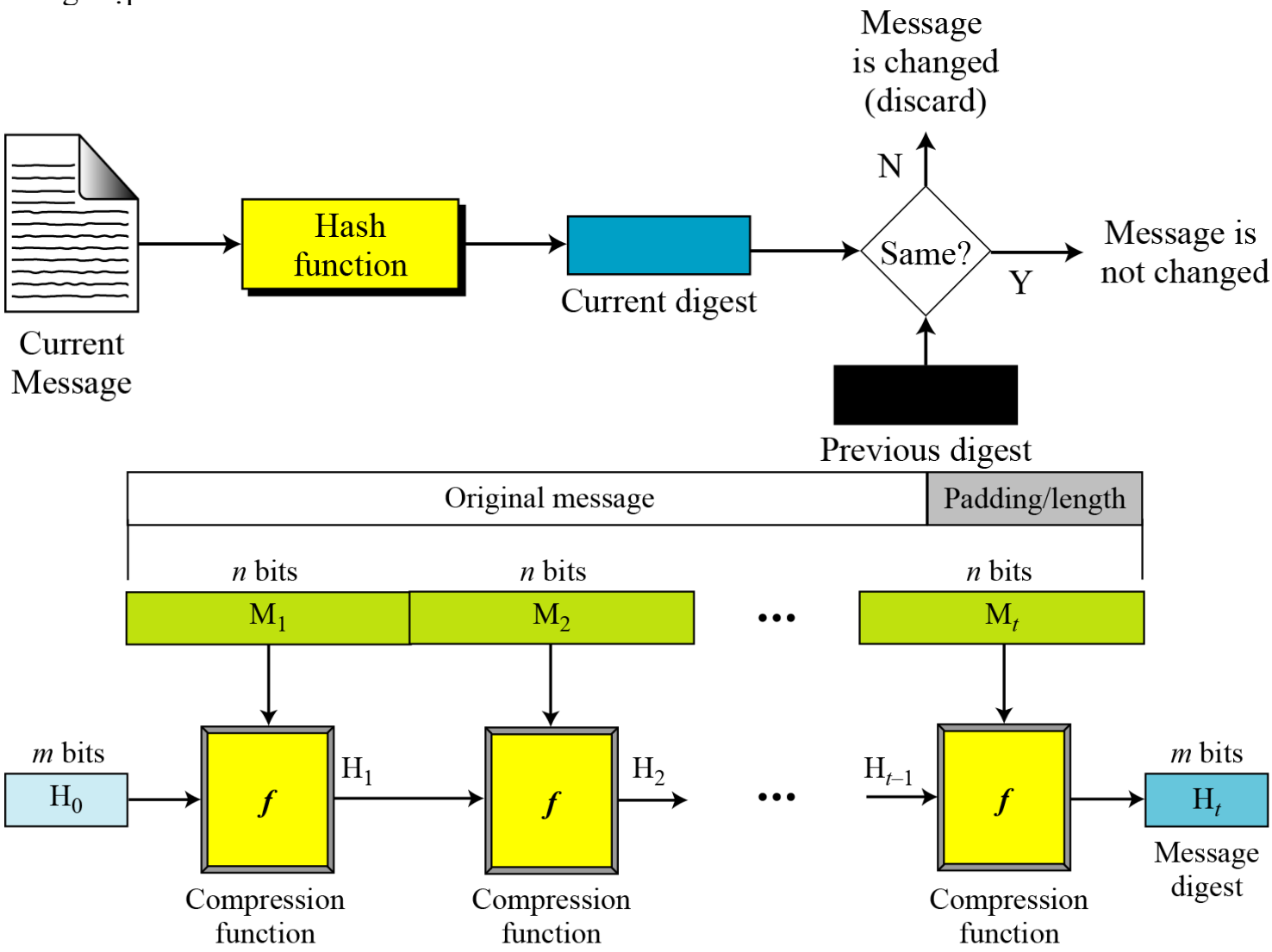
a. Trình bày các đặc điểm của hàm băm

• Hàm băm là các thuật toán nhằm phát sinh ra các giá trị băm ứng với mỗi khối dữ liệu/thông điệp.

• Giá trị băm đóng vai trò gần như là một khóa để phân biệt các khối dữ liệu/thông điệp.

• Hàm băm có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán h một chiều nào đó, rồi đưa ra một giá trị băm - bản băm - văn bản đại diện - cốt thông điệp

• Giá trị băm có kích thước ngắn & cố định & duy nhất & không trùng & không thể suy ngược lại thông điệp ban đầu .



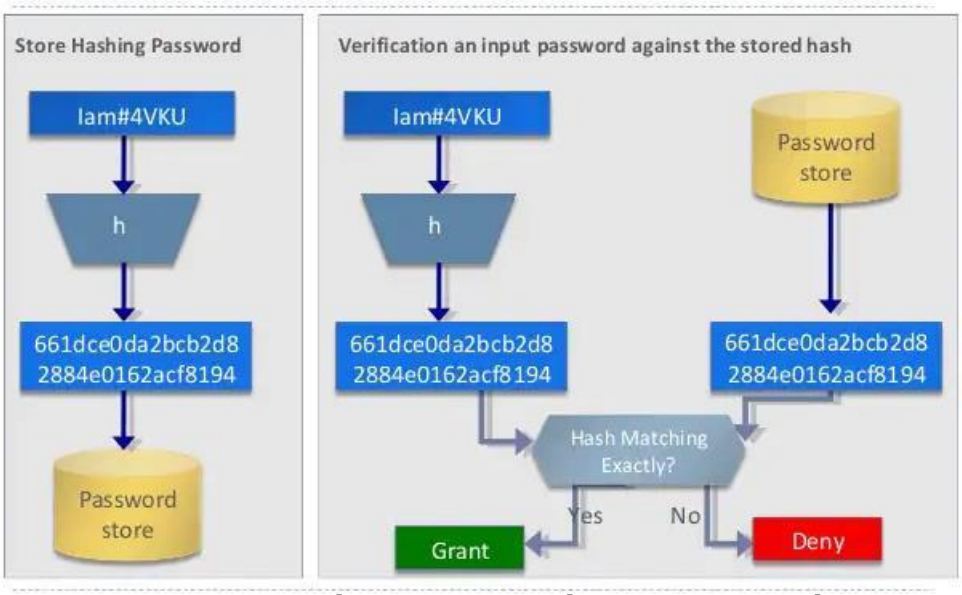
Đặc điểm

1. Tính 1 chiều (Preimage resistant – one-way property): Cho trước giá trị băm h việc tìm x sao cho H(x)=h là rất khó

2. Tính kháng đụng độ yếu (Second preimage resistant – weak collision resistance – Tính chống trùng yếu): Cho thông điệp đầu vào x, việc tìm một thông điệp x’ với (x’ khác x) sao cho h(x’)=h(x) là rất khó

3. Tính kháng đụng độ mạnh-tính chống trùng mạnh (Strong Collision resistance): Không thể tính toán để tìm được hai thông điệp đầu vào x1 khác x2 sao cho chúng có cùng giá trị băm (Nghịch lý ngày sinh – Birthday paradox)

b.Trình bày giải pháp xử lý mật khẩu trước khi lưu vào cơ sở dữ liệu và giải thích vì sao



11. SSL là gì? Tại sao cần cài SSL? Dấu hiệu nhận biết một website có cài SSL? Cách thức hoạt động của SSL?

a. SSL là gì

a. SSL (Secure Sockets Layer) là một giao thức bảo mật được sử dụng để bảo vệ các thông tin truyền qua mạng, đặc biệt là trong việc truyền dữ liệu giữa một trình duyệt web và máy chủ web. SSL đã được phát triển bởi Netscape và sau đó được tiêu chuẩn hóa thành TLS (Transport Layer Security).

Giao thức SSL/TLS sử dụng mã hóa và chứng thực để đảm bảo tính bí mật, toàn vẹn và xác thực của dữ liệu được truyền qua mạng. Khi một trình duyệt web kết nối đến một trang web sử dụng SSL/TLS, quá trình giao tiếp giữa trình duyệt và máy chủ web được mã hóa, ngăn chặn bên thứ ba không được ủy quyền từ đọc hoặc sửa đổi thông tin.

SSL/TLS sử dụng chứng chỉ số (digital certificates) để xác thực danh tính của máy chủ web. Chứng chỉ số được phát hành bởi các cơ quan chứng thực đáng tin cậy và chứa thông tin về máy chủ, bao gồm tên miền, địa chỉ IP và khóa công khai của máy chủ. Trình duyệt web sẽ kiểm tra chứng chỉ số để xác minh rằng máy chủ đích là đáng tin cậy trước khi thiết lập kết nối bảo mật.

SSL/TLS đóng vai trò quan trọng trong việc bảo vệ thông tin nhạy cảm trên Internet, bao gồm thông tin cá nhân, thông tin tài khoản ngân hàng, thông tin thẻ tín dụng và các dữ liệu quan trọng khác.

b. Tại sao cần cài SSL

1. Bảo mật dữ liệu: SSL sử dụng mã hóa để bảo vệ dữ liệu được truyền qua mạng. Khi bạn cài đặt SSL, thông tin nhạy cảm như mật khẩu, thông tin tài khoản ngân hàng, thông tin thẻ tín dụng và dữ liệu cá nhân của người dùng sẽ được mã hóa, ngăn chặn bên thứ ba không được ủy quyền từ đọc hoặc truy cập thông tin này.

2. Xác thực danh tính: SSL sử dụng chứng chỉ số (digital certificates) để xác thực danh tính của máy chủ web. Việc cài đặt SSL cho website của bạn đảm bảo rằng người dùng sẽ kết nối và tương tác với máy chủ chính xác và đáng tin cậy, ngăn chặn các cuộc tấn công giả mạo.

3. Tăng niềm tin của người dùng: Khi người dùng thấy biểu tượng "https://" và biểu tượng khóa xanh trong thanh địa chỉ trình duyệt, họ sẽ cảm thấy an tâm hơn khi truy cập và tương tác với website của bạn. SSL tạo niềm tin và uy tín, giúp xây dựng một môi trường an toàn cho khách hàng và người dùng.

4. Cải thiện SEO: Các công cụ tìm kiếm, như Google, đã công bố rằng SSL là một yếu tố tích cực ảnh hưởng đến xếp hạng trong kết quả tìm kiếm. Cài đặt SSL có thể cải thiện thứ hạng của website của bạn trong các kết quả tìm kiếm, tạo điều kiện thuận lợi hơn cho việc tìm thấy và tiếp cận từ phía người dùng.

5. Tuân thủ quy định: Trong một số lĩnh vực, như bán hàng trực tuyến hoặc thu thập thông tin nhạy cảm, việc cài đặt SSL có thể là một yêu cầu bắt buộc của luật pháp hoặc các quy định ngành. Bằng cách cài đặt SSL, bạn đảm bảo tuân thủ quy định pháp lý và tránh rủi ro pháp lý có thể phát sinh.

c. Dấu hiệu nhận biết một website có cài SSL

1. Bảo mật dữ liệu: SSL sử dụng mã hóa để bảo vệ dữ liệu được truyền qua mạng. Khi bạn cài đặt SSL, thông tin nhạy cảm như mật khẩu, thông tin tài khoản ngân hàng, thông tin thẻ tín dụng và dữ liệu cá nhân của người dùng sẽ được mã hóa, ngăn chặn bên thứ ba không được ủy quyền từ đọc hoặc truy cập thông tin này.
2. Xác thực danh tính: SSL sử dụng chứng chỉ số (digital certificates) để xác thực danh tính của máy chủ web. Việc cài đặt SSL cho website của bạn đảm bảo rằng người dùng sẽ kết nối và tương tác với máy chủ chính xác và đáng tin cậy, ngăn chặn các cuộc tấn công giả mạo.
3. Tăng niềm tin của người dùng: Khi người dùng thấy biểu tượng "https://" và biểu tượng khóa xanh trong thanh địa chỉ trình duyệt, họ sẽ cảm thấy an tâm hơn khi truy cập và tương tác với website của bạn. SSL tạo niềm tin và uy tín, giúp xây dựng một môi trường an toàn cho khách hàng và người dùng.
4. Cải thiện SEO: Các công cụ tìm kiếm, như Google, đã công bố rằng SSL là một yếu tố tích cực ảnh hưởng đến xếp hạng trong kết quả tìm kiếm. Cài đặt SSL có thể cải thiện thứ hạng của website của bạn trong các kết quả tìm kiếm, tạo điều kiện thuận lợi hơn cho việc tìm thấy và tiếp cận từ phía người dùng.
5. Tuân thủ quy định: Trong một số lĩnh vực, như bán hàng trực tuyến hoặc thu thập thông tin nhạy cảm, việc cài đặt SSL có thể là một yêu cầu bắt buộc của luật pháp hoặc các quy định ngành. Bằng cách cài đặt SSL, bạn đảm bảo tuân thủ quy định pháp lý và tránh rủi ro pháp lý có thể phát sinh.

d. Cách thức hoạt động của SSL

SSL (Secure Sockets Layer) hoạt động theo các bước sau:

1. Xác thực danh tính (Authentication): Khi một trình duyệt web kết nối đến một trang web sử dụng SSL, máy chủ sẽ gửi cho trình duyệt một chứng chỉ số (digital certificate) chứa thông tin về danh tính của máy chủ. Trình duyệt sẽ kiểm tra chứng chỉ số này để xác minh rằng máy chủ đích là đáng tin cậy và hợp lệ. Chứng chỉ số thường được phát hành bởi một cơ quan chứng thực (Certificate Authority) có uy tín.

2. Thiết lập phiên kết nối (Session Establishment): Khi xác thực được thực hiện thành công, trình duyệt và máy chủ sẽ thỏa thuận với nhau về các thông số mã hóa và giao thức bảo mật để sử dụng trong phiên kết nối. Thông thường, giao thức TLS (Transport Layer Security) được sử dụng thay thế cho SSL.

3. Giao tiếp an toàn (Secure Communication): Sau khi phiên kết nối được thiết lập, trình duyệt và máy chủ sử dụng các thuật toán mã hóa để mã hóa dữ liệu được truyền qua mạng. Mã hóa đảm bảo rằng dữ liệu không thể bị đọc hoặc sửa đổi bởi bên thứ ba khi đang truyền trên đường truyền.

4. Xác thực hai chiều (Two-way Authentication, tùy chọn): Trong một số trường hợp, SSL cũng cho phép xác thực hai chiều, nghĩa là cả trình duyệt và máy chủ đều xác thực danh tính của mình. Điều này đảm bảo rằng cả hai bên đều được xác định và tin cậy trong quá trình giao tiếp.

5. Kết thúc phiên kết nối (Session Termination): Khi quá trình giao tiếp hoàn thành, hoặc khi phiên kết nối được đóng, trình duyệt và máy chủ sẽ chấm dứt phiên kết nối. Các tài nguyên và thông tin được giải phóng, và quá trình này có thể được lặp lại khi có yêu cầu mới.

12. Tường lửa là gì? Có mấy loại và nêu tác dụng của tuần loại?

a. Tường lửa

- Tường lửa (Firewall) là một phần mềm hoặc phần cứng thiết kế để bảo vệ mạng máy tính khỏi các mối đe dọa từ bên ngoài. Nó hoạt động bằng cách kiểm soát và giám sát lưu lượng mạng đi vào và đi ra khỏi mạng, dựa trên các quy tắc được đặt trước.
- Công việc chính của tường lửa là ngăn chặn hoặc cho phép lưu lượng mạng dựa trên các quy tắc cấu hình. Các quy tắc này xác định cách thức xử lý các kết nối mạng, các giao thức được phép, các cổng mạng được mở, và các địa chỉ IP được cho phép truy cập vào hay ra khỏi mạng.
- Tường lửa có thể thực hiện các chức năng bảo mật sau:

1. Ngăn chặn truy cập từ bên ngoài: Tường lửa có thể cấu hình để chặn các kết nối không mong muốn từ bên ngoài mạng, như các cuộc tấn công mạng, tin tặc hoặc phần mềm độc hại.
2. Kiểm soát truy cập vào và ra khỏi mạng: Tường lửa có thể quản lý và kiểm soát lưu lượng mạng đi vào và đi ra khỏi mạng, đảm bảo chỉ có lưu lượng hợp lệ và an toàn được chấp nhận.
3. Mã hóa và giải mã: Tường lửa có thể hỗ trợ quá trình mã hóa và giải mã dữ liệu để bảo vệ thông tin trong quá trình truyền.
4. Xác thực người dùng: Tường lửa có thể yêu cầu người dùng xác thực trước khi cho phép truy cập vào mạng hay các dịch vụ cụ thể.
5. Giám sát và ghi lại: Tường lửa có thể giám sát và ghi lại các hoạt động mạng để phân tích, xác định các mối đe dọa và hành vi không bình thường.

Tường lửa đóng vai trò quan trọng trong việc bảo vệ mạng máy tính khỏi các cuộc tấn công, xâm nhập và sự xâm phạm vào dữ liệu quan trọng. Nó đóng gói một phần quan trọng trong kiến trúc bảo mật mạng và là một công cụ quan trọng để đảm bảo an toàn thông tin trong môi trường kết nối mạng phức tạp ngày nay.

b. Các loại tường lửa và nêu tác dụng của từ loại

Có nhiều loại tường lửa khác nhau, nhưng một số loại phổ biến nhất bao gồm:

1. Tường lửa lọc gói tin (Packet filtering firewall):

- Hoạt động bằng cách kiểm tra các gói tin dữ liệu và cho phép hoặc chặn chúng dựa trên các tiêu chí như địa chỉ IP, cổng, giao thức,...
- Ưu điểm: Dễ cài đặt và cấu hình, hiệu quả cao.
- Nhược điểm: Không thể kiểm soát lưu lượng truy cập dựa trên ứng dụng, không thể theo dõi trạng thái kết nối.

2. Tường lửa trạng thái (Stateful firewall):

- Theo dõi trạng thái của các kết nối mạng và chỉ cho phép lưu lượng truy cập hợp pháp.
- Ưu điểm: An toàn hơn tường lửa lọc gói tin, có thể theo dõi trạng thái kết nối.
- Nhược điểm: Phức tạp hơn để cài đặt và cấu hình, có thể ảnh hưởng đến hiệu suất mạng.

3. Tường lửa ứng dụng (Application-level firewall):

- Kiểm soát lưu lượng truy cập dựa trên các ứng dụng đang được sử dụng.
- Ưu điểm: Có thể kiểm soát chi tiết lưu lượng truy cập của từng ứng dụng.

- Nhược điểm: Có thể ảnh hưởng đến hiệu suất mạng, không thể bảo vệ khỏi các mối đe dọa không dựa trên ứng dụng.

4. Tường lửa proxy:

- Hoạt động như một trung gian giữa máy khách và máy chủ.
- Ưu điểm: Có thể kiểm tra và lọc lưu lượng truy cập chi tiết, ẩn địa chỉ IP của máy khách.
- Nhược điểm: Phức tạp để cài đặt và cấu hình, có thể ảnh hưởng đến hiệu suất mạng.

Tác dụng của từng loại tường lửa

1. Tường lửa lọc gói tin:

- Bảo vệ mạng khỏi các cuộc tấn công đơn giản như quét cổng, tấn công DoS cơ bản.
- Kiểm soát lưu lượng truy cập cơ bản dựa trên địa chỉ IP, cổng, giao thức.

2. Tường lửa trạng thái:

- Bảo vệ mạng khỏi các cuộc tấn công phức tạp hơn như tấn công xâm nhập, tấn công DoS nâng cao.
- Theo dõi trạng thái kết nối để ngăn chặn các gói tin trái phép.
- Kiểm soát lưu lượng truy cập dựa trên địa chỉ IP, cổng, giao thức, trạng thái kết nối.

3. Tường lửa ứng dụng:

- Bảo vệ mạng khỏi các mối đe dọa dựa trên ứng dụng như virus, phần mềm độc hại nhắm mục tiêu.
- Kiểm soát chi tiết lưu lượng truy cập của từng ứng dụng.
- Hạn chế truy cập vào các trang web và dịch vụ không phù hợp.

4. Tường lửa proxy:

- Ẩn địa chỉ IP của máy khách, bảo vệ tính riêng tư.
- Kiểm soát và lọc lưu lượng truy cập chi tiết dựa trên nội dung gói tin.
- Chặn các trang web và dịch vụ độc hại.

13. **Trình bày phương pháp phát hiện và ngăn chặn/tiêu diệt mã độc của phần mềm Antivirus? Qua đó giải thích vì sao phải thường xuyên cập nhật phần mềm Antivirus?**

a. Trình bày phương pháp phát hiện và ngăn chặn/tiêu diệt mã độc của phần mềm Antivirus

Phần mềm Antivirus là một phần mềm được thiết kế để phát hiện, ngăn chặn và tiêu diệt các mã độc, bao gồm virus, worms, trojans, spyware và các loại phần mềm độc hại khác. Dưới đây là phương pháp phát hiện và ngăn chặn/tiêu diệt mã độc của phần mềm Antivirus:

1. Phân tích chữ ký (Signature-based detection): Phương pháp này sử dụng các chữ ký đã biết của các loại mã độc để phát hiện và ngăn chặn chúng. Hệ thống Antivirus so sánh các tệp tin, quá trình hoặc phần mềm trên hệ thống với cơ sở dữ liệu chữ ký để tìm kiếm các đặc điểm phù hợp với mã độc đã biết.

- Ưu điểm: Nhanh chóng, hiệu quả đối với các virus đã được biết đến.
- Nhược điểm: Không thể phát hiện virus mới hoặc biến thể mới của virus cũ.

2. Phân tích hành vi (Behavior-based detection): Phương pháp này giám sát các hoạt động của các tệp tin, quá trình hoặc phần mềm trên hệ thống để phát hiện các hành vi đáng ngờ hoặc không bình thường. Nếu một chương trình hoặc tệp tin thực hiện các hoạt động không phù hợp hoặc độc hại, Antivirus có thể xác định và ngăn chặn chúng.

- Ưu điểm: Có thể phát hiện virus mới và biến thể mới của virus cũ.
- Nhược điểm: Có thể tạo ra kết quả dương tính giả, làm chậm hiệu suất máy tính.

3. Phân tích heuristics (Heuristic-based detection): Phương pháp này dựa trên các thuật toán và quy tắc thông minh để phát hiện các loại mã độc mới hoặc không rõ ràng. Hệ thống Antivirus phân tích các tính năng, hành vi và cấu trúc của các tệp tin hoặc phần mềm để xác định xem chúng có khả nghi hay không.
4. Công nghệ sandbox (Sandboxing): Phương pháp này chạy các tệp tin hoặc phần mềm đáng ngờ trong một môi trường cô lập được gọi là "sandbox" để quan sát hành vi của chúng mà không gây ảnh hưởng đến hệ thống chính. Nếu chúng được xác định là độc hại, Antivirus sẽ ngăn chặn chúng.
- Ưu điểm: Bảo vệ máy tính khỏi virus ngay khi nó xâm nhập.
- Nhược điểm: Có thể ảnh hưởng đến hiệu suất máy tính.

Ví dụ: Một phần mềm Antivirus phát hiện một tệp tin có chữ ký tương tự với một loại virus đã biết. Khi người dùng cố gắng mở tệp tin này, Antivirus sẽ ngăn chặn hành động và cảnh báo cho người dùng về sự tồn tại của virus.

b. Lý do phải thường xuyên cập nhật phần mềm Antivirus

Phần mềm Antivirus cần được thường xuyên cập nhật vì các mối đe dọa và mã độc mới được phát hiện liên tục. Cập nhật phần mềm Antivirus giúp:
1. Cung cấp cơ sở dữ liệu chữ ký mới: Các cập nhật định kỳ cung cấp chữ ký mới cho các loại mã độc đã biết, giúp phần mềm Antivirus phát hiện và ngăn chặn các mối đe dọa mới nhất.
2. Nâng cao khả năng phát hiện: Cập nhật phần mềm Antivirus cũng cải thiện các thuật toán phát hiện, heuristics và phân tích hành vi để tăng khả năng phát hiện các mối đe dọa mới và không rõ ràng.
3. Sửa các lỗ hổng bảo mật: Các cập nhật cũng bao gồm việc vá các lỗ hổng bảo mật trong phần mềm Antivirus, giúp ngăn chặn các cuộc tấn công từ các mối đe dọa mới sử dụng các lỗ hổng này.
4. Đảm bảo tính tương thích: Cập nhật phần mềm Antivirus cũng đảm bảo tính tương thích với các phiên bản mới của hệ điều hành và các ứng dụng khác trên hệ thống, đảm bảo hiệu suất và bảo mật tốt nhất.
Ngoài ra, việc cập nhật phần mềm antivirus còn giúp:

- Tăng cường hiệu suất: Các bản cập nhật phần mềm antivirus thường bao gồm các cải tiến hiệu suất giúp phần mềm antivirus hoạt động nhanh hơn và hiệu quả hơn.
- Sửa lỗi: Các bản cập nhật phần mềm antivirus thường bao gồm các bản sửa lỗi cho các lỗi đã biết có thể ảnh hưởng đến hiệu suất hoặc bảo mật của phần mềm antivirus.

Vì vậy, việc thường xuyên cập nhật phần mềm Antivirus là rất quan trọng để đảm bảo rằng hệ thống của bạn được bảo vệ khỏi các mối đe dọa mới và tiềm ẩn.

14. Ransomware là gì? Cách thức hoạt động và giải pháp bảo vệ dữ liệu trước Ransomware?

a. Ransomware

- Ransomware là một loại phần mềm độc hại (malware) mà mục đích chính của nó là tống tiền (ransom) từ người dùng bằng cách mã hóa dữ liệu quan trọng trên hệ thống của họ và yêu cầu một khoản tiền chuộc để khôi phục lại dữ liệu. Đây là một hình thức tấn công mạng nguy hiểm và ngày càng phổ biến.
- Khi một hệ thống bị nhiễm ransomware, phần mềm độc hại sẽ tiến hành mã hóa các tệp tin quan trọng trên máy tính hoặc mạng, bao gồm hình ảnh, tài liệu văn bản, cơ sở dữ liệu, video và các tệp tin khác. Sau khi mã hóa, ransomware sẽ hiển thị thông báo yêu cầu tiền chuộc trên màn

hình của người dùng và cung cấp hướng dẫn về cách thanh toán số tiền nhất định, thường là bằng tiền điện tử như Bitcoin.
- Mục tiêu của ransomware là buộc người dùng phải trả một khoản tiền để nhận khóa giải mã hoặc công cụ giải mã từ kẻ tấn công. Nếu người dùng không trả tiền, tệp tin của họ sẽ vẫn bị mã hóa và không thể truy cập được.
- Ransomware có thể lây lan qua email độc hại, tải xuống từ các trang web độc hại, tận dụng các lỗ hổng bảo mật hoặc sử dụng kỹ thuật xâm nhập qua mạng (network intrusion techniques). Một lần bị nhiễm ransomware, các hệ thống và dữ liệu quan trọng có thể bị hủy hoại hoặc không thể khôi phục được mà không có khóa giải mã.
- Để bảo vệ chống lại ransomware, người dùng cần thực hiện các biện pháp bảo mật như cập nhật phần mềm, sử dụng phần mềm diệt virus và tường lửa, đề phòng email độc hại và khai thác lỗ hổng bảo mật, sao lưu dữ liệu quan trọng và hạn chế quyền truy cập và chia sẻ tệp tin.
- Một số ví dụ về ransomware nổi tiếng:
1. WannaCry: WannaCry là một loại ransomware lan truyền một cách rộng rãi vào năm 2017. Nó lợi dụng một lỗ hổng bảo mật trong hệ điều hành Windows và tự động mã hóa dữ liệu trên hệ thống bị nhiễm. Ransomware này yêu cầu các nạn nhân trả tiền chuộc bằng Bitcoin để nhận được khóa giải mã.

2. Petya/NotPetya: Petya và NotPetya là hai biến thể ransomware khác nhau nhưng có cách thức hoạt động tương tự. Chúng cũng lợi dụng các lỗ hổng bảo mật trong Windows và sau khi nhiễm, chúng mã hóa bộ khởi động của hệ điều hành và các tệp tin quan trọng khác. Ransomware này cũng yêu cầu tiền chuộc để khôi phục dữ liệu.
3. Locky: Locky là một loại ransomware phổ biến đã xuất hiện vào năm 2016. Nó lan truyền qua email độc hại và sử dụng các tệp tin đính kèm được camouflaged như các tệp tin hóa đơn hay tài liệu quan trọng. Khi tệp tin đính kèm được mở, Locky sẽ mã hóa dữ liệu trên hệ thống và yêu cầu tiền chuộc.
4. Ryuk: Ryuk là một dạng ransomware được sử dụng trong các cuộc tấn công mục tiêu và yêu cầu số tiền chuộc lớn. Nó thường được triển khai sau khi hệ thống bị nhiễm malware kiểu botnet và tấn công mạng nội bộ. Ryuk phục thuộc vào việc mã hóa tệp tin quan trọng như hình ảnh, tài liệu và cơ sở dữ liệu, và yêu cầu một khoản tiền chuộc cao.

b. Cách thức hoạt động và giải pháp bảo vệ dữ liệu trước Ransomware
Ransomware hoạt động theo các bước chung sau đây:
1. Phát tán: Ransomware thường được phát tán qua email độc hại, tệp tin tải xuống từ các trang web độc hại, lợi dụng các lỗ hổng bảo mật, hoặc thông qua các kỹ thuật xâm nhập qua mạng.
2. Xâm nhập: Khi một hệ thống bị nhiễm ransomware, phần mềm độc hại tiến hành xâm nhập và lây nhiễm các tệp tin trên hệ thống. Điều này có thể bao gồm việc sử dụng các phương pháp khai thác lỗ hổng bảo mật, tấn công qua mạng hoặc sử dụng phần mềm độc hại khác để mở cửa từ bên trong hệ thống.
3. Mã hóa dữ liệu: Ransomware sẽ tiến hành mã hóa các tệp tin quan trọng trên hệ thống bị nhiễm. Quá trình này sẽ biến các tệp tin thành dạng không thể đọc được hoặc thay đổi đuôi mở rộng của chúng.
4. Yêu cầu tiền chuộc: Sau khi mã hóa dữ liệu, ransomware sẽ hiển thị thông báo yêu cầu tiền chuộc trên màn hình của người dùng. Thông báo này thường chứa hướng dẫn về cách thanh toán tiền chuộc và cung cấp thông tin liên lạc để người dùng có thể liên hệ với kẻ tấn công.
5. Chuộc giải mã: Nếu người dùng chấp nhận trả tiền chuộc, kẻ tấn công sẽ cung cấp một khóa giải mã hoặc công cụ giải mã để khôi phục dữ liệu bị mã hóa. Tuy nhiên, không có đảm bảo rằng kẻ tấn công sẽ thực sự cung cấp khóa giải mã sau khi nhận được tiền.

Một số giải pháp bảo vệ dữ liệu để đề phòng ransomware:

1. Sao lưu dữ liệu: Quan trọng nhất là thực hiện sao lưu định kỳ và đảm bảo rằng bạn có bản sao dự phòng của dữ liệu quan trọng. Sao lưu này nên được lưu trữ ngoại tuyến hoặc trên các thiết bị không kết nối mạng để tránh việc mã hóa dữ liệu sao lưu bởi ransomware.
2. Cập nhật phần mềm: Hãy đảm bảo rằng hệ điều hành và phần mềm trên hệ thống của bạn luôn được cập nhật mới nhất. Các bản cập nhật thường bao gồm các bản vá lỗi và lỗ hổng bảo mật, giúp ngăn chặn các cuộc tấn công ransomware sử dụng các lỗ hổng này.
3. Sử dụng phần mềm diệt virus và tường lửa: Cài đặt và duy trì phần mềm diệt virus/anti-malware và tường lửa mạnh mẽ trên hệ thống của bạn. Cập nhật thường xuyên và quét hệ thống để phát hiện và loại bỏ ransomware.
4. Cẩn trọng với email và tệp tin không rõ nguồn gốc (tiếp):
5. Cẩn trọng với email và tệp tin không rõ nguồn gốc: Đừng mở các tệp tin đính kèm hoặc nhấp vào các liên kết trong email không được yêu cầu hoặc không rõ nguồn gốc. Đây là phương pháp phổ biến để phát tán ransomware. Hãy kiểm tra kỹ thông tin và nguồn gốc của các email và tệp tin trước khi tương tác với chúng.
6. Giáo dục và nhận thức người dùng: Đào tạo người dùng về các mối đe dọa của ransomware và cách phòng ngừa chúng là rất quan trọng. Người dùng nên được hướng dẫn không mở tệp tin hoặc liên kết không an toàn, không tiết lộ thông tin cá nhân quan trọng và báo cáo ngay lập tức bất kỳ hoạt động nghi ngờ nào.
7. Sử dụng phần mềm chống ransomware: Có sẵn một số phần mềm chống ransomware trên thị trường. Các công cụ này có thể giúp ngăn chặn, phát hiện và chặn các cuộc tấn công ransomware bằng cách theo dõi hoạt động đáng ngờ và chặn các quy trình độc hại.
8. Thiết lập quyền truy cập và phân quyền: Hạn chế quyền truy cập của người dùng trên hệ thống để giảm khả năng lây lan của ransomware trong trường hợp một người dùng bị nhiễm.
9. Theo dõi và phát hiện sớm: Triển khai các công cụ giám sát và phát hiện sớm để phát hiện các hoạt động bất thường trên hệ thống. Việc phát hiện sớm ransomware giúp ngăn chặn sự lan truyền và giảm thiểu thiệt hại.

Câu hỏi LO5 tham khảo:

Tình huống 1:

Để phục vụ cho nhu cầu học tập và tra cứu của cán bộ, giảng viên và sinh viên của trường, nhà trường đã xây dựng một Hệ thống thư viện trực tuyến www.thuviendientu.iuh.edu.vn, hệ thống giúp độc giả (cán bộ, giảng viên và sinh viên của trường) có thể tìm kiếm các loại sách, báo, tạp chí,… Đối với tài liệu điện tử thì độc giả có thể đọc trực tuyến hoặc tải về, đối với sách trong thư viện thì độc giả có thể đăng ký mượn. Độc giả cũng có thể yêu cầu mua các loại tài liệu điện tử và thanh toán phí mua trực tuyến. Hệ thống cũng giúp cho các thủ thư có thể quản lý thông tin mượn và trả sách của độc giả, hệ thống còn có tính năng thông báo nhắc nhở đến hạn trả sách bằng email, tạo báo cáo, thống kê.

Yêu cầu: Với tình huống đã cho, bạn hãy

1. Chỉ ra ít nhất 2 loại thông tin / dữ liệu / chức năng nào cần nâng cao tính an toàn thông tin và nêu lý do tại sao?

- **Thông tin cá nhân của độc giả:** Bao gồm họ tên, địa chỉ, số điện thoại, email, thông tin tài khoản,... Đây là những thông tin nhạy cảm có thể bị lạm dụng cho mục đích đánh cắp danh tính, lừa đảo hoặc các hành vi phi pháp khác.
- **Dữ liệu về tài khoản thanh toán:** Thông tin này bao gồm số thẻ thanh toán, mã bảo mật, thông tin ngân hàng, và thông tin thanh toán khác. Bảo vệ thông tin này quan trọng để ngăn chặn việc truy cập trái phép, lừa đảo và đánh cắp tiền bạc đối với chủ sở hữu.

2. Đưa ra giải pháp nào để cài đặt nâng cao tính an toàn cho từng loại thông tin/dữ liệu/chức năng ở trên và nêu lý do tại sao phương pháp pháp này là hữu hiệu.

Đối với thông tin cá nhân của độc giả:

- Mã hóa dữ liệu: Áp dụng các thuật toán mã hóa mạnh mẽ như AES, RSA để mã hóa thông tin cá nhân của độc giả khi lưu trữ và truyền tải.
- Quản lý truy cập: Hạn chế quyền truy cập vào thông tin cá nhân chỉ dành cho những người có thẩm quyền và có nhu cầu thiết yếu.
- Bảo mật tài khoản: Yêu cầu người dùng sử dụng mật khẩu mạnh, áp dụng xác thực đa yếu tố (MFA) và thường xuyên thay đổi mật khẩu.
- Nâng cao nhận thức người dùng: Tổ chức các khóa đào tạo, hội thảo để nâng cao nhận thức của người dùng về an ninh mạng và cách thức bảo vệ thông tin cá nhân.

Đối với dữ liệu tài chính của độc giả:

- Sử dụng cổng thanh toán uy tín: Chọn lựa các cổng thanh toán uy tín, có chứng chỉ bảo mật PCI DSS để đảm bảo an toàn giao dịch trực tuyến.
- Mã hóa giao dịch: Áp dụng các giao thức bảo mật như SSL/TLS để mã hóa dữ liệu tài chính trong quá trình thanh toán.

- Giám sát gian lận: Triển khai hệ thống giám sát gian lận để phát hiện và ngăn chặn các giao dịch bất thường.
- Lưu trữ dữ liệu an toàn: Lưu trữ dữ liệu tài chính tại các trung tâm dữ liệu an toàn, có biện pháp bảo vệ vật lý và kỹ thuật chặt chẽ.

Lý do cho các giải pháp trên:

- Mã hóa dữ liệu: Giúp bảo vệ dữ liệu khỏi truy cập trái phép, ngay cả khi kẻ tấn công xâm nhập được vào hệ thống.
- Quản lý truy cập: Hạn chế rủi ro rò rỉ dữ liệu do truy cập trái phép.
- Bảo mật tài khoản: Giúp bảo vệ tài khoản người dùng khỏi bị tấn công và đánh cắp thông tin.
- Nâng cao nhận thức người dùng: Giúp người dùng hiểu rõ tầm quan trọng của bảo mật thông tin và biết cách tự bảo vệ mình.
- Cổng thanh toán uy tín: Đảm bảo an toàn cho giao dịch thanh toán trực tuyến.
- Mã hóa giao dịch: Bảo vệ dữ liệu tài chính khỏi bị trong quá trình truyền tải.
- Giám sát gian lận: Phát hiện và ngăn chặn kịp thời các hành vi gian lận.
- Lưu trữ dữ liệu an toàn: Bảo vệ dữ liệu tài chính khỏi mất mát hoặc bị đánh cắp do các sự cố về an ninh vật lý hoặc kỹ thuật.

Tình huống 2:

Để phục vụ nhu cầu học tập và nghiên cứu của cán bộ, giảng viên và sinh viên của trường (gọi chung là độc giả), nhà trường đã trang bị một phòng đọc sách cho các độc giả. Phòng này có trang bị máy lạnh, bàn ghế, wifi, và 100 chiếc máy tính để bàn. Sinh viên có thể tự vào ra phòng đọc sách trong khoảng thời gian thư viện mở để ngồi đọc sách, học tập nghiên cứu và dùng các máy tính. Các máy tính chỉ dùng để học tập/nghiên cứu chứ không cho phép chơi game.

Yêu cầu:

1. Theo bạn để có thể kiểm soát, chứng thực và theo dõi sự vào ra phòng đọc sách của các độc giả một cách tự động thì chúng ta có thể dùng phương pháp nào để kiểm soát và nêu lý do tại sao phương pháp này là hữu hiệu?

1. Kiểm soát và chứng thực sự ra vào phòng đọc sách:

Phương pháp đề xuất: Sử dụng hệ thống thẻ từ kết hợp camera giám sát.

Lý do:

- Hiệu quả: Hệ thống thẻ từ cho phép ghi nhận chính xác thời gian ra vào của từng độc giả, đồng thời camera giám sát có thể xác minh danh tính và đảm bảo an ninh.
- Tiện lợi: Sử dụng thẻ từ đơn giản, nhanh chóng, không cần tiếp xúc trực tiếp với nhân viên, phù hợp với lượng lớn người sử dụng.
- Bảo mật: Thẻ từ có thể được mã hóa để đảm bảo tính an toàn và tránh giả mạo.
- Quản lý dữ liệu: Hệ thống có thể ghi chép dữ liệu ra vào tự động, giúp theo dõi số lượng người sử dụng, thời gian sử dụng và lập báo cáo thống kê.

2. Theo bạn để có thể chứng thực, kiểm soát và theo dõi việc sử dụng wifi và thiết bị máy móc ở phòng đọc sách thì chúng ta dùng những phương pháp nào và nêu lý do tại sao phương pháp này là hữu hiệu?

2. Chứng thực, kiểm soát và theo dõi việc sử dụng wifi và thiết bị máy tính:

Phương pháp đề xuất:

- Kết hợp hệ thống quản lý mạng (NMS) và phần mềm giám sát máy tính:
  - NMS cho phép quản trị viên theo dõi lưu lượng truy cập mạng, lọc các trang web độc hại, chặn các ứng dụng chơi game và quản lý băng thông cho từng người dùng.
  - Phần mềm giám sát máy tính ghi lại hoạt động của người dùng trên máy tính, bao gồm các chương trình sử dụng, thời gian sử dụng và các tệp tin truy cập.
- Cài đặt phần mềm chống virus và phần mềm chống phần mềm độc hại:
  - Bảo vệ thiết bị khỏi các mối đe dọa an ninh mạng và đảm bảo an toàn cho dữ liệu của người dùng.

Lý do:

- Hiệu quả: Giúp quản trị viên kiểm soát hiệu quả việc sử dụng wifi và thiết bị máy tính, đảm bảo an ninh mạng và ngăn chặn các hoạt động vi phạm quy định.
- Linh hoạt: Có thể cấu hình hệ thống để phù hợp với nhu cầu cụ thể của phòng đọc sách, ví dụ như giới hạn thời gian sử dụng máy tính cho mỗi người dùng hoặc chỉ cho phép truy cập vào các trang web học tập.
- Dễ dàng quản lý: Quản trị viên có thể theo dõi và quản lý hệ thống từ xa thông qua giao diện web hoặc ứng dụng di động.

Tình huống 3:

Một trang web có đường link xem chi tiết sản phẩm như sau:

www.trangthuongmaidientu.com/sanpham.php?id_sanpham=2

Yêu cầu:

1. Theo bạn, cách truyền biến như trang web có đường link trên dễ bị loại tấn công hay lỗ hổng gì? Giải thích vì sao?

Phân tích lỗ hổng:

Cơ chế truyền biến sử dụng trong đường link www.trangthuongmaidientu.com/sanpham.php?id_sanpham=2 tiềm ẩn các lỗ hổng bảo mật sau:

- Tấn công tiêm mã độc (XSS): Kẻ tấn công có thể chèn mã độc hại vào giá trị id_sanpham để thực thi khi người dùng truy cập trang web. Ví dụ, kẻ tấn công có thể thay thế id_sanpham=2 bằng id_sanpham=script%3Ealert(document.cookie)%3C/script>, khiến trình duyệt thực thi mã JavaScript độc hại, đánh cắp thông tin cookie của người dùng.

- Tấn công truy cập trái phép (SQL Injection): Kẻ tấn công có thể chèn truy vấn SQL độc hại vào giá trị id_sanpham để truy cập trái phép vào cơ sở dữ liệu của trang web. Ví dụ, kẻ tấn công có thể thay thế id_sanpham=2 bằng id_sanpham=-1;SELECT%20*%20FROM%20users;--, khiến truy vấn SQL SELECT * FROM users được thực thi, tiết lộ thông tin người dùng.
- Tấn công đoán mật khẩu (Brute-force attack): Kẻ tấn công có thể thử nhiều giá trị id_sanpham khác nhau để đoán ID sản phẩm hợp lệ. Việc thiếu cơ chế bảo vệ có thể khiến kẻ tấn công dễ dàng truy cập vào trang sản phẩm và thực hiện các hành vi độc hại.

2. Trình bày giải pháp khắc phục cho loại tấn công hoặc lỗ hổng trên?

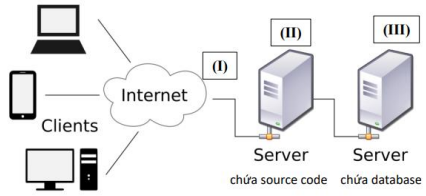
Để khắc phục các lỗ hổng bảo mật trên, cần áp dụng các biện pháp sau:

- Sử dụng phương thức POST thay vì GET: Thay vì truyền dữ liệu nhạy cảm trên thanh địa chỉ, phương thức POST sẽ gửi dữ liệu trong body của yêu cầu HTTP, giúp bảo mật thông tin tốt hơn.
- Sử dụng tham số hóa truy vấn: Thay vì chèn trực tiếp giá trị id_sanpham vào truy vấn SQL, hãy sử dụng tham số hóa để tách biệt dữ liệu người dùng khỏi truy vấn. Việc này giúp ngăn chặn các truy vấn SQL độc hại được thực thi.
- Kiểm tra và lọc dữ liệu đầu vào: Cần kiểm tra và lọc cẩn thận dữ liệu đầu vào (id_sanpham) để loại bỏ các ký tự đặc biệt và mã độc hại trước khi xử lý.
- Sử dụng token chống giả mạo (CSRF): Token CSRF giúp bảo vệ trang web khỏi các yêu cầu giả mạo do kẻ tấn công gửi đi.
- Hạn chế quyền truy cập cơ sở dữ liệu: Chỉ cung cấp cho ứng dụng web quyền truy cập vào các bảng dữ liệu cần thiết, hạn chế tối đa khả năng truy cập trái phép.
- Cập nhật phần mềm thường xuyên: Cần cập nhật thường xuyên hệ thống quản trị nội dung (CMS) và các phần mềm liên quan để vá các lỗ hổng bảo mật mới nhất.

Bằng cách áp dụng các giải pháp trên, trang web có thể tăng cường bảo mật và giảm thiểu nguy cơ bị tấn công.

Tình huống 4:

Cho một hệ thống thông tin đơn giản sau:



Yêu cầu:

Trình bày các giải pháp giúp tăng cường độ an toàn cho hệ thống tại các điểm I (đường truyền), II (server chứa source) và III (server chứa database)? Giải thích vì sao?

Mô hình client server

Mô hình Client Server là mô hình mạng máy tính trong đó các máy tính con được đóng vai trò như một máy khách, chúng làm nhiệm vụ gửi yêu cầu đến các máy chủ. Để máy chủ xử lý yêu cầu và trả kết quả về cho máy khách đó.

- **Client:** Đây là nơi gửi đi các yêu cầu đến server bằng cách tổ chức giao tiếp giữa người dùng, server và môi trường bên ngoài. Client sẽ tiến hành tiếp nhận yêu cầu của người dùng và thành lập các chuỗi truy vấn để gửi đến máy chủ. Khi nhận được kết quả từ server, Client sẽ tiến hành hiển thị kết quả đó cho người truy cập.
- **Server:** Nhiệm vụ của server là xử lý những yêu cầu được Client gửi đến. Sau khi tiến hành xử lý, server sẽ gửi trả lại kết quả đến Client để Client tiếp tục xử lý kết quả và phục vụ nhu cầu của người dùng.

Giải pháp tại điểm I

1. Tấn công tại đường truyền:

- **Tấn công từ chối dịch vụ (DoS):** Kẻ tấn công tràn ngập máy chủ bằng lưu lượng truy cập giả mạo, khiến máy chủ quá tải và không thể phục vụ các yêu cầu hợp pháp.
- **Tấn công "người thứ ba" (MitM):** Kẻ tấn công chặn đường truyền giữa máy khách và máy chủ, đánh cắp dữ liệu hoặc sửa đổi thông tin trao đổi.
- **Tấn công đánh cắp dữ liệu:** Kẻ tấn công sử dụng các kỹ thuật như sniffing hoặc eavesdropping để lấy cắp dữ liệu nhạy cảm được truyền tải trên mạng.

Bảo vệ đường truyền:

- Sử dụng tường lửa để chặn các truy cập trái phép và tấn công DoS.
- Sử dụng giao thức HTTPS để mã hóa dữ liệu để bảo vệ thông tin khi truyền tải trên mạng.
- Cài đặt chứng chỉ SSL cho website để xác thực danh tính của website và bảo vệ người dùng khỏi các website giả mạo.
- Cài đặt phần mềm chống virus và phần mềm chống phần mềm độc hại trên máy khách và máy chủ.

2. Tấn công tại máy chủ chứa source:

- Tấn công SQL injection: Kẻ tấn công chèn mã độc hại vào truy vấn SQL để truy cập trái phép vào cơ sở dữ liệu hoặc thực thi các lệnh trên máy chủ.
- Tấn công Cross-Site Scripting (XSS): Kẻ tấn công chèn mã JavaScript độc hại vào trang web, khiến người dùng khi truy cập trang web bị thực thi mã độc.
- Tấn công zero-day: Kẻ tấn công khai thác lỗ hổng bảo mật chưa được nhà cung cấp phần mềm vá lỗi.

Bảo vệ máy chủ chứa source:

- Sử dụng mật khẩu mạnh và bảo mật thông tin đăng nhập, yêu cầu phải có ít nhất 8 ký tự bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.
- Hạn chế quyền truy cập vào máy chủ chỉ cho những người dùng cần thiết.
- Sử dụng các truy vấn SQL có tham số và sử dụng hàm prepared statement để ngăn chặn kẻ tấn công chèn mã độc hại vào truy vấn.
- Cập nhật phần mềm máy chủ web và cơ sở dữ liệu thường xuyên để vá các lỗ hổng bảo mật.

3. Tấn công tại máy chủ chứa database:

- Tấn công brute force: Kẻ tấn công thử đoán mật khẩu truy cập vào cơ sở dữ liệu bằng cách sử dụng nhiều tổ hợp mật khẩu khác nhau.
- Tấn công denial-of-service (DoS): Kẻ tấn công tràn ngập cơ sở dữ liệu bằng các truy vấn giả mạo, khiến cơ sở dữ liệu quá tải và không thể phục vụ các truy vấn hợp pháp.
- Tấn công SQL injection: Kẻ tấn công chèn mã độc hại vào truy vấn SQL để truy cập trái phép vào cơ sở dữ liệu hoặc thực thi các lệnh trên máy chủ.

Bảo vệ server database:

- Sử dụng mã hóa dữ liệu để bảo vệ thông tin lưu trữ trong cơ sở dữ liệu.
- Cài đặt hệ thống quản lý truy cập cơ sở dữ liệu (DBMS) mạnh mẽ và cấu hình quyền truy cập hợp lý.
- Sao lưu dữ liệu thường xuyên bằng các công cụ như như pgBadger hoặc MySQL Enterprise Backup và lưu trữ bản sao lưu ở nơi an toàn.

Ngoài ra, cần triển khai các biện pháp bảo mật chung như:

- Nâng cao nhận thứ về an ninh mạng cho người dùng.
- Thực hiện các bài tập luyện tập và kiểm tra an ninh mạng thường xuyên.
- Có kế hoạch phản ứng sự cố để xử lý các vi phạm an ninh mạng kịp thời.

1. Điều khiển truy cập là gì? Trình bày các phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.

Điều khiển truy cập là quá trình giới hạn *quyền sử dụng* của người dùng đã được chứng thực đối với *tài nguyên hệ thống*, cũng như hạn chế các tác động của người dùng đối với tài nguyên hệ thống và đảm bảo người dùng chỉ tác động được các tài nguyên trong phạm vi được cấp quyền đó.

- **Access control gồm:**
  - **Các đối tượng cần Bảo vệ (Protect objects):** bảo vệ các tài nguyên hệ thống
    - ví dụ, tài nguyên bộ nhớ, tập tin, thư mục, tài nguyên phần cứng, phần mềm, bảng, các bộ, ...
  - **Chủ thể (subjects)**: các đơn vị hoạt động yêu cầu truy cập đến tài nguyên,
    - ví dụ, người sử dụng, chủ sở hữu, chương trình, vv
  - **Chế độ truy cập (access mode)**: các kiểu truy cập
    - ví dụ, đọc / select, viết / cập nhật, thực thi.

Chức năng của access control

- Cấp phép hoặc từ chối phê duyệt sử dụng các tài nguyên xác định cho các chủ thể
- Kiểm soát được các đối tượng đang hoạt động hay các đối tượng có thể bị truy cập bởi các hoạt động khác.

Các phương pháp điều khiển truy cập

- Điều khiển truy cập tùy ý (Discretionary Access Control)
  - Cho biết chủ thể nào có thể truy cập kiểu gì đến các đối tượng trong CSDL
  - Có những nguyên tắc một chủ thể có thể tùy ý cấp quyền hay lấy lại quyền truy cập hoặc gián tiếp đến lớp dữ liệu
  - Là mô hình cởi mở nhất
- Điều khiển truy cập bắt buộc (Mandatory Access Control)
  - Là mô hình nghiêm ngặt nhất
  - Định trước các nguyên tắc để chủ thể (thuộc 1 lớp) truy cập trực tiếp hoặc gián tiếp đến các lớp dữ liệu
- Điều khiển truy cập dựa trên vai trò (Role Based Access Control)
  - Vai trò là 1 tập các quyền. Không thực hiện cấp quyền cho từng chủ thể mà gán cho chủ thể 1 vai trò, khi đó chủ thể sẽ có tất cả các quyền thuộc về vai trò đó
  - Là mô hình được sử dụng thực tế nhất
- Điều khiển truy cập dựa trên qui tắc (Rule Based Access Control)
  - Tự động gán vai trò cho các chủ thể dựa trên một tập quy tắc do người giám sát xác định
  - Mỗi đối tượng tài nguyên chứa các thuộc tính truy cập dựa trên quy tắc
  - Khi người dùng truy cập tới tài nguyên, hệ thống sẽ kiểm tra các qui tắc của đối tượng để xác định quyền truy cập
  - Thường được sử dụng để quản lý truy cập người dùng tới một hoặc nhiều hệ thống

Câu hỏi dạng 2) Điều khiển truy cập là gì? Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.

Điều khiển truy cập là quá trình giới hạn *quyền sử dụng* của người dùng đã được chứng thực đối với *tài nguyên hệ thống*, cũng như hạn chế các tác động của người dùng đối với tài nguyên hệ thống và đảm bảo người dùng chỉ tác động được các tài nguyên trong phạm vi được cấp quyền đó.

- **Access control gồm:**
  - **Các đối tượng cần Bảo vệ (Protect objects):** bảo vệ các tài nguyên hệ thống
    - ví dụ, tài nguyên bộ nhớ, tập tin, thư mục, tài nguyên phần cứng, phần mềm, bảng, các bộ, ...
  - **Chủ thể (subjects)**: các đơn vị hoạt động yêu cầu truy cập đến tài nguyên,
    - ví dụ, người sử dụng, chủ sở hữu, chương trình, vv
  - **Chế độ truy cập (access mode)**: các kiểu truy cập
    - ví dụ, đọc / select, viết / cập nhật, thực thi.

Chức năng của access control

- Cấp phép hoặc từ chối phê duyệt sử dụng các tài nguyên xác định cho các chủ thể
- Kiểm soát được các đối tượng đang hoạt động hay các đối tượng có thể bị truy cập bởi các hoạt động khác.

Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.

1) Điều khiển truy cập bắt buộc (Mandatory Access Control-MAC)
   - Là mô hình điều khiển truy cập nghiêm ngặt nhất
   - Thường bắt gặp trong các thiết lập của quân đội
   - Hai thành phần: Nhãn và Cấp độ
- Mô hình MAC cấp quyền bằng cách đối chiếu nhãn của đối tượng với nhãn của chủ thể
  - Nhãn cho biết cấp độ quyền hạn
- Người dùng và dữ liệu được phân loại dựa theo các lớp bảo mật (security classes).
- Phân loại **người dùng** dựa theo mức **độ tin cậy** và lĩnh vực hoạt động của người dùng.
- Phân loại **dữ liệu** dựa theo mức **độ nhạy cảm** và lĩnh vực của dữ liệu
- Lớp bảo mật có thể được phân loại theo
  - Mức bảo mật (Classification level)
  - Lĩnh vực (Category)

- **Các mức bảo mật cơ bản:**
  - Không phân loại (U – Unclassified)
  - Bí Mật (C – Confidential)
  - Tuyệt mật (S – Secret)
  - Tối mật (TS – Top Secret)
- Trong đó TS là mức cao nhất và U là mức thấp nhất:

  TS > S > C > U
- Người dùng ở **cấp càng cao** thì mức độ đáng **tin cậy càng lớn**. Dữ liệu ở **cấp càng cao** thì **càng nhạy cảm** và cần được bảo vệ nhất.

Ưu điểm:

- Là cơ chế điều khiển truy xuất có tính bảo mật cao trong việc ngăn chặn dòng thông tin bất hợp pháp.
- Thích hợp cho các ứng dụng trong môi trường quân đội.

Khuyết điểm:

- Không dễ áp dụng: đòi hỏi cả người dùng và dữ liệu phải được phân loại rõ ràng
- Chỉ được ứng dụng trong một số ít môi trường.
- Phức tạp
- Làm giảm tính linh hoạt của hệ thống (ảnh hưởng đến hiệu năng)

Phương pháp 2

- Điều khiển truy cập tùy ý (Discretionary Access Control)
  - Cho biết chủ thể nào có thể truy cập kiểu gì đến các đối tượng trong CSDL
  - Có những nguyên tắc một chủ thể có thể tùy ý cấp quyền hay lấy lại quyền truy cập hoặc gián tiếp đến lớp dữ liệu
  - Là mô hình cởi mở nhất
- **Quyền hạn (permission): c**hỉ cấp cho user chính xác những quyền mà user cần đến. Việc cấp dư thừa những quyền không cần thiết có thể gây nguy hại cho việc bảo mật hệ thống.
- Role là một tập hợp bao gồm các quyền và các role khác. Role được gán cho các user hoặc các role khác. Role giúp cho việc quản trị người dùng dễ dàng và tiết kiệm công sức hơn.

Ưu điểm

- Phù hợp với hầu hết các ứng dụng trong thực tế.
- Mô hình đơn giản, hiệu quả.
- Đơn giản trong việc quản lý permission, thay vì quản lý permission trên từng user ta sẽ quản lý permission trên mỗi nhóm.Việc này giúp giảm công sức, thời gian cũng như giảm rủi ro nhầm lẫn.
- Mô hình RBAC phân cấp hỗ trợ sự phân cấp vai trò (Role hierarchies) với mối quan hệ cha con, theo đó tất cả quyền hạn của role cha được kế thừa bởi role con.Điều này ngăn cản sự bùng nổ role và tăng khả năng sử dụng lại trong mô hình RBAC.

Hạn chế:

- Không phù hợp với một số tài nguyên cần bảo vệ là chưa biết trước.
- Không phù hợp khi quy tắc điều khiển truy cập phức tạp, việc điều khiển truy cập không chỉ dựa vào thông tin về vai trò, mà còn phụ thuộc vào các thông tin ngữ cảnh khác.
- Không phù hợp với các ứng dụng mà một người dùng có thể mang nhiều vai trò mâu thuẫn với nhau. Điều này phần nào được giải quyết với mô hình RBAC ràng buộc tĩnh hay động.Tuy nhiên khi các quy tắc đảm bảo tính loại trừ là phức tạp và chưa biết trước thì RBAC ràng buộc không đáp ứng được hoặc khó cài đặt.