Goi YTra Loi Cau Hoi On Tap CK Nmattt

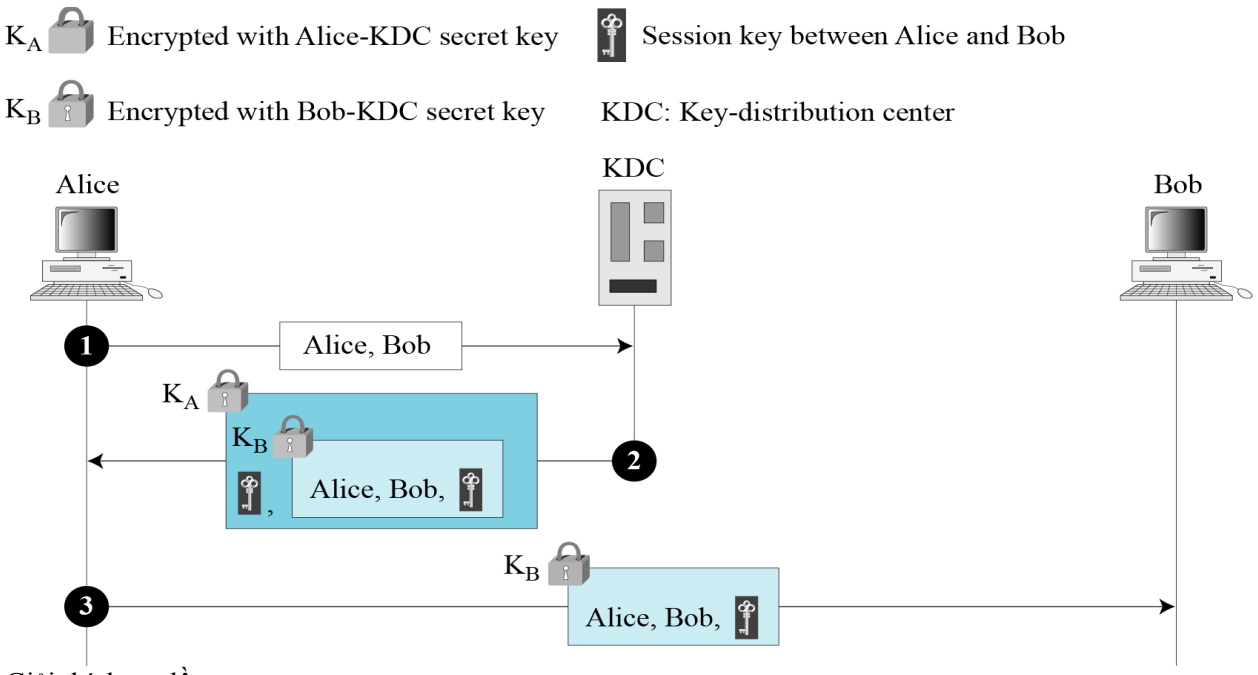
Công Nghệ Phần Mềm (Trường Đại học Công nghiệp Thành phố Hồ Chí Minh)

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.**

- KDC tạo khóa bí mật cho mỗi thành viên, khóa bí mật này chỉ có thể dùng giữa thành viên và KDC, chứ không dùng giữa hai thành viên
- Nếu muốn dùng giữa hai thành viên, KDC tạo một ***session key*** giữa hai thành viên, sử dụng khóa của họ với trung tâm.
- ***Khóa phiên giữa hai thanh viên chỉ được dùng một lần*** (sau giao tiếp kết thúc thì khóa phiên cũng không còn tác dụng)

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.

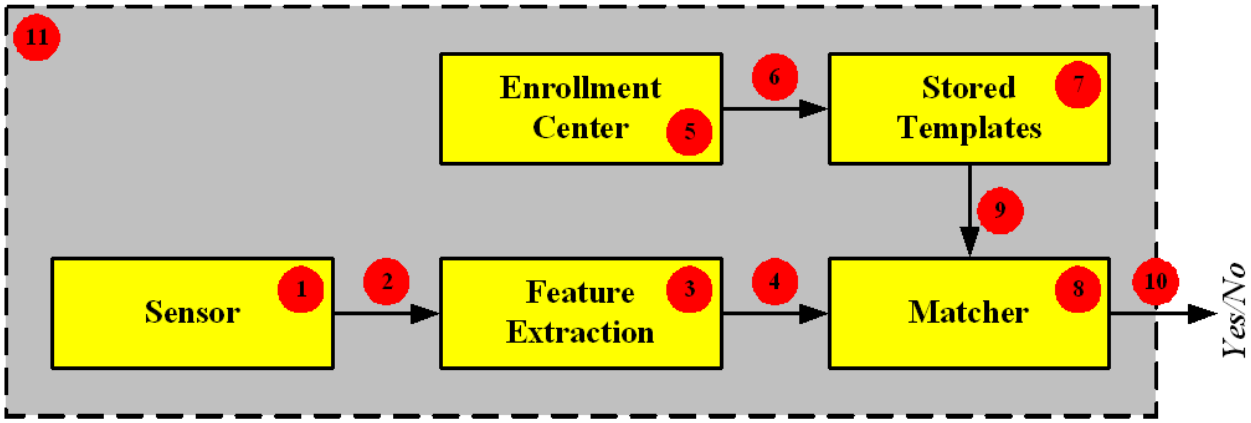


Giải thích sơ đồ

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?

- 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.

Qui trình xác thực bằng Biometrics



Giải thích

Các thành phần cần quan tâm trong quy trình xác thực bằng sinh trắc học:

- Components (thành phần) : Vài Component cần cho sinh trắc học, bao gồm:
    - các thiết bị thu nhận đặc tính của sinh trắc học
    - Chương trình xử lý các đặc tính sinh trắc học
    - Các thiết bị lưu trữ.
- 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 tin 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
- Accuracy (độ chính xác) : Độ chính xác (Accuracy) của các kỹ thuật sinh trắc học được đo lường bằng cách dùng hai tham số:
    - **False Rejection Rate (FRR)**
    - **False Acceptance Rate (FAR)**
- Applications (các ứng 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 điểm bán (trả tiền) điều tra bằng cách phân tích AND hoặc vân tay
- **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 sẵn 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

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

---

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.**
   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.

   - Một hệ thống điều khiển truy cập có 3 cách kiểm soát khác nhau:
       - Truy cập chính sách (access control *policy),*
       - Mô hình điều khiển truy cập (access control *model)*
       - Cơ chế điều khiển truy cập (access control *mechanism)*.

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 tùy ý - Discretionary Access Control (DAC)** chỉ rõ những đặc quyền mà mỗi chủ thể có thể có được trên các đối tượng và trên hệ thống (object privilege, system privilege)
- **Sức mạnh của DAC:** Tính linh hoạt là một lý do chính tại sao nó được biết đến rộng rãi và được thực hiện trong các hệ thống điều hành chủ đạo.
    - Người dùng có thể bảo vệ những gì thuộc về mình
    - Chủ của dữ liệu có toàn quyền trên dữ liệu đó
    - Chủ của dữ liệu có quyền định nghĩa các loại truy cập đọc/ghi/thực thi và gán những quyền đó cho những người khác

Điều khiển truy cập của DAC trong một hệ CSDL là dựa vào 2 thao tác cơ bản:

- **Gán quyền (granting privileges):** Cho phép người dùng khác được quyền truy cập lên đối tượng do mình làm chủ. Tuy nhiên, trong DAC có thể lan truyền các quyền.
- **Thu hồi quyền (revoking privileges):** thu hồi lại quyền đã gán cho người dùng khác

Các qui tắc trao quyền

- Các yêu cầu và chính sách an toàn do tổ chức đưa ra, người trao quyền có nhiệm vụ chuyển các yêu cầu này thành các quy tắc trao quyền
- **Qui tắc trao quyền:** biểu diễn đúng với môi trường phần mềm/phần cứng bảo vệ.
- **Quyền ở cấp tài khoản/hệ thống (account/system level):** là những quyền độc lập với các đối tượng trong hệ CSDL. Những quyền này do người quản trị hệ thống định nghĩa và gán cho mỗi người dùng
- ***Quyền ở cấp đối tượng(object level)***: là những quyền trên mỗi đối tượng trong hệ CSDL. Người dùng tạo ra đối tượng nào thì sẽ có tất cả các quyền trên đối tượng đó.

Ưu điểm

- Mô hình ít hạn chế nhất
- Mọi đối tượng đều có một chủ sở hữu
- Chủ sở hữu có toàn quyền điều khiển đối với đối tượng của họ
- Chủ sở hữu có thể cấp quyền đối với đối tượng của mình cho một chủ thể khác
- Được sử dụng trên các hệ điều hành như Microsoft Windows và hầu hết các hệ điều hành UNIX
- Dễ dàng thực hiện, hệ thống linh hoạt
- DAC linh động trong chính sách nên được hầu hết các HQT CSDL ứng dụng

Nhược điểm

- Phụ thuộc vào quyết định của người dùng để thiết lập cấp độ bảo mật phù hợp
    - Việc cấp quyền có thể không chính xác

→Khó quản lý việc gán / thu hồi quyền

- ❖ Quyền của chủ thể sẽ được "thừa kế" bởi các chương trình mà chủ thể thực thi

→Dễ bị lộ thông tin

- ❖ Không thể thiếu được dòng thông tin (information flow control) để có thể chống lại tấn công dạng Trojan Horse
- ❖ Kiểm soát an toàn không tốt

- 2.2. Điều khiển truy cập dựa trên vai trò (Rule Based Access Control-RBAC)
  - ❑ 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 quy 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
    - Những thay đổi trong doanh nghiệp có thể làm cho việc áp dụng các quy tắc thay đổi

Có 2 loại quyền:

- **Quyền hệ thống (System Privilege):**
  - Là quyền thực hiện một tác vụ CSDL cụ thể hoặc quyền thực hiện một loại hành động trên tất cả những đối tượng schema của hệ thống.
- **Quyền đối tượng (Schema Object Privilege hoặc Object Privilege):**
  - Là quyền thực hiện một hành động cụ thể trên một đối tượng schema cụ thế.
  - Có nhiều quyền đối tượng khác nhau dành cho các loại đối tượng schema khác nhau.
  - Dùng để quản lý việc truy xuất đến các đối tượng schema cụ thể nào đó

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.

Nhược điểm:

- 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.

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.

Mật khẩu: 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**

Fixed password	One-time password

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.

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.

- Ưu và nhược điểm:…..

TOKEN KEY (TOKEN CARD)

- Là thiết bị bảo mật mà doanh nghiệp
- cung 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.
- Ưu và nhược điểm:…..
-

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.
- Ưu và nhược điểm:…..

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.

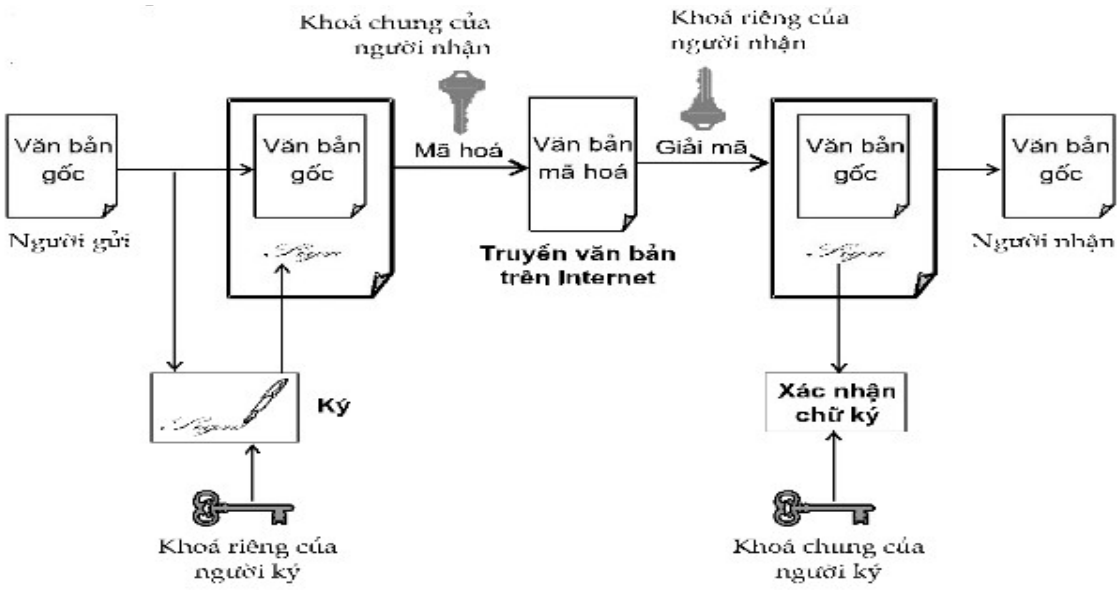
----Cho vi dụ, mô tả các bước, chỉ ra bước nào chứng thực.

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

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.

- 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 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.
- Nó có vai trò như chữ ký đối với cá nhân hay con dấu đối với tổ chức, doanh nghiệp và dùng để xác nhận lời cam kết của tổ chức, cá nhân đó trong văn bản mình đã ký trên môi trường điện tử số. Chữ ký số được được thừa nhận về mặt pháp lý.

Hoặc định nghĩa theo khoản 1 Điều 21 Luật Giao dịch điện tử năm 2005.



Giải thích sơ đồ tạo và kiểm tra chữ ký số: …..

Mục tiêu của chữ ký số;

- **Xác thực (Authentication):** giải thích xác thực cái gì
- **Chống phủ nhận (Non-repudiation):** Giải thích chống thoái thác như thế nào

Hiện trạng áp dụng chữ ký: 4 lĩnh vực đó là cơ quan Thuế, Bảo hiểm xã hội, Hải quan và Chứng khoán.

- Cơ quan Thuế

- Tính đến 31/3/2019, số lượng DN đã đăng ký tham gia sử dụng dịch vụ với cơ quan thuế là 703.753 DN (không bao gồm các đơn vị chi nhánh, trực thuộc) trên tổng số 711.748 DN đang hoạt động, đạt tỷ lệ 98,87%.

  Dùng ký số vào chức năng nào…..

- **Bảo hiểm xã hội,**
  …….
- **Hải quan**
  …….
- **Chứng khoán.**
  ……

7. **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?**

- 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)

Mục tiêu của chứng thư số?

- Xác thực
- Chống thống thác
- Đảm bảo tính bí mật, toàn vẹn

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

- Slide 78,79

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

- 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***

Mục tiêu của hệ thống an toàn thông tin:

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

- Hệ thống quản lý an toàn thông tin (ISMS) duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin bằng cách áp dụng một quá trình quản lý rủi ro và mang lại sự tin cậy cho các bên quan tâm rằng các rủi ro đã được quản lý đầy đủ.

- 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 hoạt động nghiệp vụ thường ngày; Các sự cố ATTT do người dùng gây ra sẽ được hạn chế tối đa khi nhân viên được đào tạo, nâng cao nhận thức ATTT.
- Giúp hoạt động đảm bảo ATTT luôn được duy trì và cải tiến. Các biện pháp kỹ thuật và chính sách tuân thủ được xem xét, đánh giá, đo lường hiệu quả và cập nhật định kỳ.
- Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến ATTT.
- Nâng cao uy tín của tổ chức, tăng sức cạnh tranh, tạo lòng tin với khách hàng, đối tác, thúc đẩy quá trình toàn cầu hóa và tăng cơ hội hợp tác quốc tế

9. 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?

- 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

- Tính 1 chiều (Preimage resistant – one-way property):
    a. Cho trước giá trị băm h việc tìm x sao cho H(x)=h là rất khó
- Tính kháng đụng độ yếu (Second preimage resistant – weak collision resistance – Tính chống trùng yếu):
    a. Cho thông điệp đầu vào x, việc tìm một thông điệp x’ với (x’≠ x) sao cho h(x’)=h(x) là rất khó
- Tính kháng đụng độ mạnh-tính chống trùng mạnh (Strong Collision resistance):
- Không thể tính toán để tìm được hai thông điệp đầu vào $x_1 \neq x_2$ sao cho chúng có cùng giá trị băm (Nghịch lý ngày sinh – Birthday paradox)

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

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?

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?

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?

1. Tấn công người chơi giữa (Man-in-the-Middle): Khi thông tin được truyền qua mạng, một kẻ tấn công có thể can thiệp vào quá trình truyền thông và đánh cắp hoặc thay đổi dữ liệu truyền đi. Đường link trên trong truyền biến có thể bị tấn công này, vì thông tin được truyền qua đường link và có thể bị thay đổi trên đường đi.

2. Tấn công gửi tin giả mạo (Spoofing): Kẻ tấn công có thể tạo ra một đường link giả mạo, tức là một đường link giống hệt đường link trang web chính, nhằm đánh lừa người dùng. Khi người dùng nhấp vào đường link giả mạo, kẻ tấn công có thể thu thập thông tin nhạy cảm hoặc tiến hành các hành động gian lận.

3. Tấn công xâm nhập SQL (SQL injection): Nếu truyền biến trên đường link được sử dụng để tạo câu truy vấn SQL mà không được kiểm tra và xử lý đúng cách, kẻ tấn công có thể chèn các đoạn mã độc vào câu truy vấn. Điều này có thể cho phép kẻ tấn công thực hiện các thao tác không được ủy quyền, truy cập dữ liệu nhạy cảm hoặc thậm chí kiểm soát toàn bộ hệ thống.

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

Để giảm thiểu các lỗ hổng và tấn công liên quan đến truyền biến như trang web có đường link trên, hãy thực hiện các biện pháp sau:

- Sử dụng kết nối bảo mật HTTPS để mã hóa thông tin truyền qua đường link, từ đó giảm thiểu nguy cơ bị tấn công người chơi giữa.

- Xác thực và kiểm tra đầu vào từ người dùng. Hãy đảm bảo rằng các thông tin được truyền qua đường link không chứa mã độc hoặc các ký tự đặc biệt có thể gây lỗi hoặc tấn công.

- Sử dụng cơ chế xử lý dữ liệu an toàn, như sử dụng thủ tục lưu trữ thích hợp để tránh tấn công xâm nhập SQL.

- Luôn cập nhật và áp dụng các bản vá bảo mật cho trang wed và các thành phần liên quan , để giảm thiểu rủi ro từ các lỗ hỏng đã biết .

- Đào tạo người dùng để nhận biết và tránh nhấp vào các đường link đáng ngờ hoặc không xác định nguồn gốc

Tuy nhiên, cần lưu ý rằng an toàn thông tin là một lĩnh vực phức tạp và liên tục thay đổi. Việc áp dụng các biện pháp bảo mật phù hợp và duy trì cập nhật là rất quan trọng để bảo vệ truyền biến trên đường link.

3. Tìm hiểu trên mạng xem cách khắc phục tấn công SQL Injection nhé

Để khắc phục tấn công SQL Injection, có một số biện pháp và kỹ thuật phổ biến được khuyến nghị bởi các chuyên gia bảo mật. Dưới đây là một số cách khắc phục tấn công SQL Injection:

1. Sử dụng câu truy vấn tham số hóa (Parameterized Queries) hoặc truy vấn chuẩn (Prepared Statements): Thay vì tạo truy vấn SQL bằng cách ghép chuỗi, sử dụng câu truy vấn tham số hóa hoặc truy vấn chuẩn. Điều này cho phép cung cấp các tham số truy vấn riêng biệt, và hệ thống sẽ xử lý các giá trị này một cách an toàn, loại bỏ khả năng thực hiện SQL Injection.

2. Kiểm tra và làm sạch đầu vào: Trước khi sử dụng đầu vào từ người dùng trong câu truy vấn SQL, hãy kiểm tra và làm sạch đầu vào để loại bỏ hoặc vô hiệu hóa các ký tự đặc biệt có thể gây ra lỗ hổng SQL Injection. Có thể sử dụng các hàm an toàn như escape hoặc quote để tránh việc xâm nhập SQL.

3. Hạn chế quyền truy cập cơ sở dữ liệu: Cấu hình quyền truy cập cơ sở dữ liệu sao cho các tài khoản có ít quyền truy cập nhất cần thiết để thực hiện các tác vụ cần thiết. Điều này giảm thiểu tác động của SQL Injection, ngay cả khi tấn công thành công, bởi vì kẻ tấn công chỉ có thể thực hiện các tác vụ theo quyền hạn của tài khoản đó.

4. Cập nhật phần mềm và áp dụng bản vá bảo mật: Đảm bảo rằng hệ thống và các thành phần liên quan được cập nhật đầy đủ và áp dụng các bản vá bảo mật mới nhất. Nhà cung cấp phần mềm thường phát hiện và vá các lỗ hổng SQL Injection trong quá trình phát triển, do đó việc cập nhật đều đặn là cần thiết.

5. Sử dụng các công cụ bảo mật: Có sẵn các công cụ bảo mật chuyên dụng để phát hiện và ngăn chặn tấn công SQL Injection. Các công cụ này có thể phân tích và kiểm tra các câu truy vấn SQL tự động để tìm ra các lỗ hổng có thể bị

tấn công.

6. Đào tạo và nâng cao nhận thức an ninh: Đào tạo nhân viên về an ninh thông tin và tạo ý thức về các mối đe dọa SQL Injection. Nhân viên nên được hướng dẫn về việc kiểm tra và xác minh đầu vào, sử dụng các phương pháp an toàn và báo cáo các vấn đề an ninh liên quan.

Đây chỉ là một số cách khắc phục tấn công SQL Injection phổ biến. Tuy nhiên, mỗi hệ thống có đặc điểm riêng, và việc áp dụng các biện pháp bảo mật phụ thuộc vào tình huống cụ thể và các yêu cầu của hệ thống.

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?

Loại thông tin/dữ liệu/chức năng cần nâng cao tính an toàn thông tin:

a) Thông tin đăng nhập và quản lý tài khoản người dùng: Đây là loại thông tin nhạy cảm, bao gồm tên đăng nhập, mật khẩu và thông tin cá nhân của cán bộ, giảng viên và sinh viên. Nâng cao tính an toàn thông tin trong việc quản lý tài khoản người dùng là rất quan trọng để đảm bảo rằng chỉ có người dùng được ủy quyền mới có thể truy cập và thực hiện các hoạt động trong hệ thống.

b) Thông tin giao dịch tài chính: Bao gồm thanh toán phí mua tài liệu điện tử và quản lý thông tin liên quan đến giao dịch tài chính. Thông tin này cần được bảo vệ chặt chẽ để đảm bảo tính toàn vẹn và bảo mật của các giao dịch tài chính, tránh rủi ro mất cắp thông tin tài chính hoặc gian lận giao dịch.

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.

2. Giải pháp nâng cao tính an toàn thông tin cho từng loại thông tin/dữ liệu/chức năng:

a) Thông tin đăng nhập và quản lý tài khoản người dùng:
- Sử dụng mã hóa mật khẩu: Lưu trữ mật khẩu dưới dạng mã hóa thay vì dạng văn bản thô, sử dụng thuật toán bảo mật như bcrypt để mã hóa mật khẩu. Điều này giúp ngăn chặn việc đọc trực tiếp mật khẩu trong trường hợp dữ liệu bị xâm nhập.
- Xác thực hai yếu tố (2FA): Để tăng cường bảo mật, triển khai xác thực hai yếu tố như mã xác thực động qua điện thoại di động hoặc ứng dụng xác thực để đảm bảo rằng chỉ người dùng đúng mới có thể truy cập vào hệ thống.

b) Thông tin giao dịch tài chính:
- Sử dụng giao thức bảo mật HTTPS: Đảm bảo rằng toàn bộ giao dịch tài chính diễn ra qua kênh an toàn, sử dụng HTTPS để mã hóa dữ liệu trong quá trình truyền tải.
- Quản lý và lưu trữ thông tin tài chính an toàn: Áp dụng các biện pháp bảo vệ dữ liệu tài chính, bao gồm mã hóa, cơ chế kiểm soát truy cập và sao lưu định kỳ, để đảm bảo tính bảo mật và khả dụng của dữ liệu tài chính.

***Lý do cho sự hiệu quả của các phương pháp trên:**
- Mã hóa mật khẩu và xác thực hai yếu tố giúp ngăn chặn việc truy cập trái phép vào tài khoản người dùng, ngay cả khi dữ liệu bị xâm nhập.
- Sử dụng giao thức bảo mật HTTPS đảm bảo tính toàn vẹn và bảo mật của dữ liệu giao dịch trong quá trình truyền tải.
- Quản lý và lưu trữ thông tin tài chính an toàn giúp đảm bảo tính bảo mật và khả dụng của dữ liệu tài chính, tránh mất cắp thông tin và gian lận giao dịch.

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?
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?

1. Để kiểm soát, chứng thực và theo dõi sự vào ra phòng đọc sách của các độc giả một cách tự động, chúng ta có thể sử dụng hệ thống quản lý thẻ thông minh (RFID - Radio Frequency Identification). Mỗi độc giả sẽ được cấp một thẻ thông minh chứa thông tin cá nhân và mã định danh riêng. Các cửa vào phòng đọc sách sẽ được trang bị cảm biến RFID để đọc thông tin từ thẻ khi độc giả tiến vào hoặc ra khỏi phòng.

Lý do tại sao phương pháp này hữu hiệu:
- Tiện lợi: Độc giả chỉ cần mang theo thẻ thông minh và tiến vào phòng, không cần tương tác với nhân viên thư viện. Điều này giúp tiết kiệm thời gian và làm giảm tình trạng xếp hàng tại quầy lễ tân.
- Chính xác và nhanh chóng: Hệ thống RFID có thể đọc thông tin từ thẻ một cách chính xác và nhanh chóng, cho phép xác định ngay lập tức sự vào ra của độc giả.
- Tự động: Hệ thống này hoạt động tự động và không đòi hỏi sự can thiệp thủ công, giúp tiết kiệm nhân lực và tối ưu quy trình quản lý phòng đọc sách.

2. Để chứng thực, kiểm soát và theo dõi việc sử dụng wifi và thiết bị máy móc ở phòng đọc sách, chúng ta có thể sử dụng hệ thống quản lý mạng và giám sát truy cập.

- Quản lý mạng: Sử dụng phần mềm quản lý mạng để kiểm soát việc truy cập vào wifi trong phòng đọc sách. Chỉ cho phép độc giả có quyền truy cập vào mạng khi họ đã đăng nhập thành công bằng tài khoản và mật khẩu riêng.
- Giám sát truy cập: Thiết lập hệ thống giám sát mạng và ghi lại hoạt động truy cập internet của từng thiết bị. Điều này cho phép nhà trường theo dõi việc sử dụng wifi và phát hiện sự lạm dụng hoặc truy cập không đúng mục đích.

Lý do tại sao phương pháp này hữu hiệu:
- Bảo mật: Hệ thống quản lý mạng và chứng thực wifi giúp đảm bảo chỉ có người d

ùng được ủy quyền mới có thể truy cập vào mạng. Điều này giúp ngăn chặn truy cập trái phép và đảm bảo an ninh thông tin.
- Quản lý: Giám sát truy cập mạng và ghi lại hoạt động giúp nhà trường có cái nhìn tổng quan về việc sử dụng wifi và thiết bị máy móc ở phòng đọc sách. Điều này hỗ trợ quản lý tài nguyên, xác định nhu cầu và thực hiện các biện pháp quản lý hiệu quả hơn.

Tổng cộng, việc sử dụng hệ thống quản lý thẻ thông minh và hệ thống quản lý mạng giúp kiểm soát, chứng thực và theo dõi sự vào ra phòng đọc sách cũng như việc sử dụng wifi và thiết bị máy móc một cách tự động và hiệu quả.