An toàn thông tin- GVHD: TS Ngô Hữu Dũng

Nội dung LO3 - Giải thích được các khái niệm cơ bản về An toàn thông tin, hệ mã hóa

1. Chữ ký điện tử là gì? Mục tiêu của chữ ký điện tử? Trình bày hiện trạng áp dụng chữ ký điện tử ở Việt Nam

- Định nghĩa: Chữ ký điện tử hay còn gọi là chữ ký số là một thiết bị được mã hóa tất cả các dữ liệu, thông tin của một doanh nghiệp dùng thay cho chữ kí trên các loại văn bản và tài liệu số thực hiện đối với các giao dịch điện tử qua mạng internet.

- Mục tiêu của chữ ký điện tử

+Xác thực (Authentication)

+Chống phủ nhận (Non-repudiation)◊

->Chữ ký số không những giúp xác thực thông điệp mà còn bảo vệ mỗi bên khỏi bên kia.

(gợi ý: Định nghĩa chữ ký điện tử: ứng dụng của mã hóa khóa công khai, người dùng có (PUA, PRA); Tạo chữ ký: SAM=E(M,PRA) – giải thích; Thẩm tra chữ ký D(SAM, PUA) à Yes/No (chỗ này em chưa rõ ạ) – 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)

2. Đưa ra một hệ thống thông tin hoặc một trang web thực tế ở Việt Nam mà có sử dụng chữ ký điện tử? Nghiệp vụ nào trong hệ thống đó có sử dụng chữ ký số? Trình bày các bước cụ thể để người dùng trong hệ thống này thực hiện nghiệp vụ có sử dụng chữ ký số. (gợi ý: Website của cơ quan Thuế, Website của cơ quan Hải quan, Website của cơ quan Bảo hiểm xã hội, ...)

Website của cơ quan Hải quan

Để đăng ký sử dụng chữ ký số trong thủ tục hải quan điện tử, doanh nghiệp phải có chữ ký số được cung cấp bởi các nhà cung cấp dịch vụ chữ ký số đã được Bộ Thông tin và truyền thông cấp phép.

Sau khi đã có chữ ký số, tiến hành đăng ký tại dịch vụ "Đăng ký doanh nghiệp sử dụng chữ ký số" trên Cổng TTĐT Hải quan với các bước như sau:

Bước 1: Cắm USB Token vào máy tính. Lưu ý: máy tính sử dụng để đăng ký phải được cài Java (nếu chưa có, download tại đây).

Bước 2: Đăng nhập

- Mã doanh nghiệp: nhập mã số thuế của doanh nghiệp.

- Số CMT:

+ Doanh nghiệp trong nước: số chứng minh nhân dân hoặc số hộ chiếu thể hiện trên Giấy Chứng nhận ĐKKD của doanh nghiệp.

+ Doanh nghiệp có vốn đầu tư nước ngoài: số chứng minh nhân dân hoặc số hộ chiếu của người đại diện pháp luật.

- Nhập dãy số xác nhận.

- Bấm "Xem thông tin".

Bước 3: Xác nhận thông tin đăng ký.

- Bấm "Xem thông tin chứng thư số".

- Trường hợp xảy ra lỗi: sử dụng một máy tính khác để tiến hành lại từ Bước 1.

- Trường hợp không xảy ra lỗi: hệ thống tự động lấy thông tin và hiển thị lên màn hình, nhập thông tin "Ngày hiệu lực đăng ký" và "Ngày hết hiệu lực đăng ký", bấm "Đăng ký thông tin" để hoàn thành việc đăng ký.

3. Chứng thư số là gì? Mục tiêu của chứng thư số? Hiện nay Việt Nam đã có các đơn vị nào có thể cung cấp dịch vụ chứng thư số?

*Định nghĩa

Là một văn bản cung cấp khóa công khai

được cung cấp và quản lý bởi một tổ chức gọi là nhà cung cấp chứng chỉ(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.

*Mục tiêu

Là chứng thực để gắn một chìa khóa công khai với một thực thể (cá nhân, máy chủ, cty,...). Hay nói cách khác, CTS giúp xác định chìa khóa công khai thuộc về thực thể nào.

Một CTS thường gồm chìa khóa công khai và một số thông tin khác về thực thể sở hữu chìa khóa đó.

Chứng thư số thuộc sở hữu của nhà cc chứng thư số, viết tắt CA (certificate authority).

*09 doanh nghiệp được Bộ TT & TT cấp phép triển khai dịch vụ chữ ký số công cộng bao gồm:
1.vina-ca

2.viettel-ca

3.bkav-ca

4.vnpt-ca

5.newtel-ca

6.nacencommsct-ca

7.fpt-ca

8.ck-ca

9.safecert-ca

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

*Định nghĩa

Là một văn bản cung cấp khóa công khai

được cung cấp và quản lý bởi một tổ chức gọi là nhà cung cấp chứng chỉ(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.

*Nội dung

1. Tên thuê bao

2. Số hiệu của chứng thư số (Serial)

3. Thời hạn hiệu lực của chứng thư số

4. Tên tổ chức chứng thực chữ ký số (EASYCA, VNPT-CA, CA2, BKAV-CA, VIETTEL-CA…)

5. Chữ ký số của tổ chức chứng thực chữ ký số

6. Thư hạn chế mục đích và phạm vi sử dụng của chứng thư số

7. Những hạn chế về trách nhiệm của tổ chức cung cấp dịch vụ chứng thực chữ ký số

8. Các nội dung cần thiết khác theo quy định của Bộ Thông tin& Truyền thông

5. Chứng thực thực thể là gì? Trình này 2 phương pháp mà bạn biết mà có thể cài đặt để chứng thực thực thể.

*Định nghĩa

Là một kỹ thuật được thiết kế cho phép một bên (party) chứng minh sự nhận dạng (identity) của một bên khác.

Xác thực thực thể là tạo ra liên kết giữa định danh và đối tượng, thực thể gồm 2 bước: Chủ thể cung cấp một định danh trong hệ thống , chủ thể cung cấp thông tin xác thực có thể chứng minh sự liên kết giữa định danh và chủ thể.

*2 phương pháp

- Chứng thực bằng Passwords
- Chứng thực bằng Challenge – Response
- Chứng thực Zero-Knowledge ZKP
- Chứng thực bằng sinh trắc học Biometrics.
- Ngoài ra còn có các phương pháp sử dụng kết hợp các phương pháp trên.

6. 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.

*Định nghĩa:

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

*2 phương pháp

- Chứng thực bằng Passwords
- Chứng thực bằng Challenge – Response
- Chứng thực Zero-Knowledge ZKP
- Chứng thực bằng sinh trắc học Biometrics.
- Ngoài ra còn có các phương pháp sử dụng kết hợp các phương pháp trên.

7. 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

Là phương pháp đơn giản và lâu đời nhất, được gọi là Password-based Authentication, password là một thứ mà người dùng biết.

Một Password được dùng khi một người dùng cần truy xuất một hệ thống để sử dụng nguồn tài nguyên của hệ thống.

*Mật khẩu cố định và mật khẩu dùng một lần khác nhau

Mật khẩu cố định được dùng lặp đi lặp lại cho 1 tài khoản còn mật khẩu 1 lần chỉ dùng 1 lần cho 1 lần thực hiện.

*Điểm mạnh của mật khẩu cố định

- Mất số điện thoại thì vẫn có thể đăng nhập được

- Yêu cầu khi đặt mật khẩu có nhiều ký tự khác nhau, tăng tính bảo mật

*Điểm yếu

- Con người phải ghi nhớ-> quên thì quá trình lấy lại mất khẩu tốn thời gian

- Mỗi tài khoản, yêu cầu đặt mật khẩu khác nhau làm cho người dùng dễ nhầm lẫn.

*Điểm mạnh của mật khẩu 1 lần

- Không phải ghi nhớ

- Độ bảo mật cao: có gửi mã xác nhận

*Nhược điểm

- Bị thất thoát mã OTP cho đối tượng xấu sẽ dễ bị đánh cắp thông tin.

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

- SMS OTP

Ưu: +Nhanh chóng và tiện lợi

+Phổ biến, được dùng ở các ngân hang, các trang điện tử lớn như Facebook, Google, Zalo,….

Nhược: Điện thoại mất sóng thì không nhận được mã OTP.

- Token Key (Token Card)

Ưu: + Tạo mã OTP không cần Internet, mỗi phút tạo 1 mã mới

+ Nhỏ gọn, dễ mang theo khi cần thiết.

Nhược: + 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.

+ Vì dễ mang nên cũng dễ rớt, phải cẩn thận khi mang theo.

- Smart OTP

Ưu: + 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.

Nhược: +Mất mạng thì không truy cập được app

9. Đưa ra một hệ thống mà bạn biết có sử dụng mật khẩu cố định (fixed password) và mô tả các bước thực hiện để bạn có thể được chứng thực người dùng trong hệ thống đó. Nêu mục tiêu của việc chứng thực này.

Là một password được dùng lặp đi lặp lại mỗi lần truy xuất. Được dùng trong các hệ thống có số lượng lặp đi lặp lại như: Facebook, Gmail,….

Bước 1: User ID và Password File

Để truy xuất tài nguyên, người dùng gửi bản rõ của User ID và Password đến hệ thống.

Bước 2: Hashing the password

Nếu Password trùng khớp với Password trong hệ thống, thì quyền truy xuất được gán ngược lại từ chối.

Bước 3: Salting the password

*Mục tiêu

- Xác định danh tính người dùng

- Bảo vệ quyền truy cập của người dùng

10. 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.

Mã xác thực OTP (One Time Password) là mật khẩu chỉ sử dụng một lần. Đây là hình thức bảo mật đã quá quen thuộc với tất cả chúng ta, đặc biệt là những người thường xuyên thanh toán online, giao dịch ngân hàng. Tuy nhiên, có điều mà chúng ta luôn không để ý rằng OTP còn là "mật khẩu", chỉ khác với mật khẩu mà ta tự thiết lập và ghi nhớ là mật khẩu này chỉ sử dụng "một lần" để tăng cường thêm một lớp bảo vệ cho những tài khoản quan trọng của chúng ta.

Trước 1 giao dịch chuyển tiền, các ngân hàng sẽ gửi SMS hoặc Voice OTP vào số điện thoại mà bạn đăng ký thẻ để xác nhận bạn là người chuyển chứ không phải là người khác.

Mục tiêu:

Nhằm giúp ngăn chặn, giảm thiểu những rủi ro tài khoản của bạn bị tấn công khi mật khẩu bị lộ hoặc hacker xâm nhập. Nếu không có OTP xác nhận, tài khoản của người tiêu dùng sẽ nhanh chóng bị các thành phần xấu xâm nhập và người tiêu dùng bị mất cảnh giác

11. Sinh trắc học (biometric) là gì? Nêu các lĩnh vực mà có thể áp dụng sinh trắc học?

Chứng thực thực thể bằng sinh trắc học (Biometrics) là sử dụng các phép đo lường về các đặc tính sinh lí học hoặc hành vi học mà nhận dạng một con người, các đặc thù của sinh trắc học không thể đoán , ăn cắp hay chia sẻ. ví dụ như vân tay, vân lòng bàn tay, võng mạc, móng mắt, khuôn mặt, giọng nói…

Các lĩnh vực mà có thể áp dụng sinh trắc học:

- Lĩnh vực bên cơ quan nhà nước, chính phủ

- Chăm sóc sức khỏe

- Giao thông vận tải

- Quản lý khách sạn

- Quản lý trường học

- Quản lý lực lượng lao động

12. Nêu ưu điểm và nhược điểm của việc áp dụng chứng thực bằng sinh trắc học.

Ưu điểm:

+ Có độ chính xác cao

+ thời gian chứng thực rất nhanh (nhỏ hơn 1s)

+ Sự tác động của người dùng thấp

+ Có sự kết hợp nhiều yếu tố: vân tay, võng mạc, giọng nói.

Nhược điểm:

+ Giá thành: triển khai hệ thống sinh trắc học đòi hỏi chi phí cao cho cả phần cứng (thiết bị thu/quét, và nhận dạng) với các phần mềm hiện đại.

+ có thể nhận diện sai: do hư hỏng phần cứng, lỗi phần mềm làm cho hệ thống từ chối người dùng mặc dù đúng người.

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

Khái niệm: ISMS là công cụ để các nhà lãnh đạo quản lý thực hiện 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.

Mục tiêu

+ Đảm bảo tính bí mật của thông tin, tức là thông tin chỉ được phép truy cập bởi những đối tượng được cấp phép.

+ Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

+ Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn. Ví dụ, nếu một server chỉ bị ngưng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng của nó là 99,999%.

Nội dung LO4 - Mô tả được tổng quan cơ chế/giao thức để thiết lập và nâng cao tính an toàn thông tin cho một tình huống cụ thể

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 và nêu lý do tại sao

-Hệ thống đăng nhập và hệ thống thanh toán cần nâng cao tính an toàn vì

+Hệ thống đăng nhập nếu không được bảo mật, hacker sẽ xâm nhập và đánh cắp thông tin người dùng

+Hệ thống thanh toán vì đây là nghiệp vụ liên quan đến tiền nên phải cẩn thận để tránh trường hợp rủi ro mất tiền, hoặc hệ thống bị lỗi.

2. Đưa ra giải pháp nào (chữ ký số, xác thực và điều khiểu truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngươi,…)) 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 nhất.

+Hệ thống đăng nhập cần dùng truy cập bằng mật khẩu vì

Mất số điện thoại thì vẫn có thể đăng nhập được

Yêu cầu khi đặt mật khẩu có nhiều ký tự khác nhau, tăng tính bảo mật

+Hệ thống đăng nhập bằng mật khẩu 1 lần để xác nhận giao dịch

Không phải ghi nhớ

Độ bảo mật cao: có gửi mã xác nhận

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 (chữ ký số, xác thực và điều khiểu truy cập bằng mật khẩu (fixed password, OTP), sinh trắc học (vân tay hoặc khuôn mặt, con ngươi,…)) để kiểm soát và nêu lý do tại sao phương pháp này là hữu hiệu nhất?

Dùng sinh trắc học là hiệu quả nhất vì

+ Có độ chính xác cao

+ thời gian chứng thực rất nhanh (nhỏ hơn 1s)
+ Sự tác động của người dùng thấp
+ Có sự kết hợp nhiều yếu tố: vân tay, võng mạc, giọng nói.

2. Theo bạn để có thể chứng thức, 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 (chữ ký số, xác thực và điều khiểu truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngươi,…)) và nêu lý do tại sao phương pháp này là hữu hiệu nhất?

Dùng đăng nhập bằng mật khẩu vì đây là việc sử dụng nhiều lần, lặp đi lặp lại. Tạo mật khẩu cố định dễ ghi nhớ, thuận tiện trong bảo mật cũng như an toàn cho người dùng.

Tình huống 3:

Giả sử khoa Kế toán của trường IUH trang bị một 'Phòng mô phỏng và thực hành quy trình nghiệp vụ Kế toán – Tài chính – Tín dụng' (gồm 30 máy tính) dùng để phục vụ cho việc học tập và nghiên cứu của các thành viên trong câu lạc bộ Kế_Tài_Ngân_Club. Phòng máy này gồm một máy chủ (server), nhiều máy trạm (work station) và một máy in (printer) được cài đặt các phần mềm về kế toán, tài chính & ngân hàng để cho các thành viên trong câu lạc bộ vào sử dụng để nghiên cứu và học tập. Khoa mong muốn phòng máy được cài đặt và cấu hình làm sao mà các thành viên có thể ra vào và sử dụng các tài nguyên một cách thuận tiện nhưng vẫn có cơ chế theo dõi một cách tự động.

1. Theo bạn, phòng máy nên dùng phương pháp nào (chữ ký số, xác thực và điều khiểu truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngơi,…)) mà các thành viên có thể vào ra một cách thuận tiện nhưng vẫn kiểm soát được khi cần thiết. Bạn hãy mô tả giải pháp một cách chi tiết nhất và nêu lý do tại sao đây là giải pháp hợp lý nhất.

Nên dùng mật khẩu cố định

2. Theo bạn, để có thể kiểm soát việc sử dụng thiết bị, ứng dụng được cài đặt trong phòng mô phỏng chúng ta thể dùng phương pháp nào (chữ ký số, xác thực và điều khiểu truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngơi,…)) và nêu lý do tại sao đây là giải pháp hợp lý nhất?

Mật khẩu cố định (khúc này em lười quá nên em nghĩ giải 1 tình huống là làm được rồi ạ)

Dạ em cảm ơn thầy <3