Thông tin chung về học phần

Bộ môn (Khoa phụ trách)	Khoa Công nghệ thông tin
Thuộc CTĐT	Công nghệ thông tin
Số tín chỉ	3
•Số tiết lý thuyết:	22.5
•Số tiết thực hành:	15
•Số tiết tự học:	120
Số bài kiểm tra:	1
Học phần tiên quyết:	Không
Học phần học trước:	Giải tích, Đại số tuyến tính, Toán rời rạc
Học phần song hành:	Không
Học phần liên quan:	Bảo mật ứng dụng & hệ thống; Hệ điều hành

Thông tin chung về học phần

Mô tả chung về nội dung:

- Giới thiệu các kiến thức cơ bản về an toàn và bảo mật thông tin
- Mã hoá thông tin và các phương pháp mã hoá thông tin: mã hoá cổ điển và hiện đại;
- Ứng dụng mã hoá thông tin trong thực tế: chữ kí điện tử, xác thực,…

Thông tin chung về học phần

Thông tin chung về giảng viên:

STT	Họ và tên	Địa chỉ E-mail	Ghi chú
1	PGS.TS. Nguyễn Trung Thành	thanh.nguyentrung@phenikaa-uni.edu.vn	Khoa CNTT-Phenikaa
2	TS. Phạm Thị Thanh Thủy		Học Viện An Ninh
3	TS. Đoàn Trung Sơn		Học viện An Ninh

Thông tin chung về học phần

Giá trình và tài liệu tham khảo:

[1]. Trịnh Nhật Tiến (2015), ***Nhập môn an toàn thông tin***. NXB ĐHQGHN.

[2]. Lê Đắc Nhường (2018), ***An Toàn Dữ Liệu***. NXB ĐHQGHN.

[3]. Nguyễn Khanh Văn (2019), ***Giáo trình An toàn thông tin***. NXB Bách Khoa.

[4]. Phạm Huy Điển, Hà Huy Khoái (2004), ***Mã hóa thông tin cơ sở toán học và ứng dụng***, NXB ĐHQGHN.

Thông tin chung về học phần

Điểm đánh giá:

- Điểm chuyên cần (CC) : **10%**
- Điểm đánh giá giữa kỳ : **40%**
- Điểm đánh giá cuối kỳ : **50%**

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

An toàn thông tin là gì?

Mục tiêu cơ bản của an toàn thông tin

Sự cần thiết của an toàn thông tin

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

An toàn thông tin là gì?

An toàn thông tin là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin,...

Mục tiêu cơ bản của an toàn thông tin

+ Đảm bảo tính bảo mật (**Confidentiality**)

+ Đảm bảo tính toàn vẹn (**Integrity**)

+ Đảm bảo tính sẵn sàng (**Availability**)

Information Security Attributes

+ Đảm bảo tính xác thực (**Authenticity**)

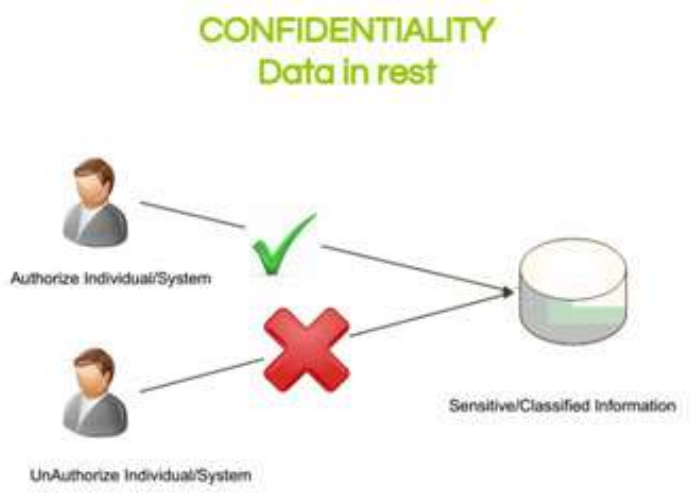
+ Đảm bảo tính không thể chối cãi (**Non repudiation**)

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Mục tiêu cơ bản của an toàn thông tin

+ Đảm bảo tính bảo mật (**Confidentiality**)

Bí mật là thuật ngữ được sử dụng để tránh lộ thông tin đến những đối tượng không được xác thực hoặc để lọt vào các hệ thống khác.

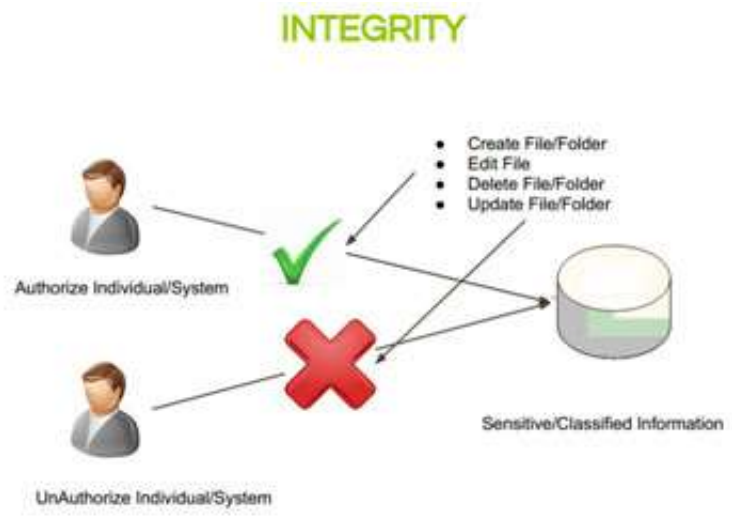


CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Mục tiêu cơ bản của an toàn thông tin

+ Đảm bảo tính toàn vẹn (**Integrity**)

Toàn vẹn có nghĩa rằng dữ liệu không thể bị chỉnh sửa mà không bị phát hiện. Tính toàn vẹn bị xâm phạm khi một thông điệp bị chỉnh sửa trong giao dịch.



CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Mục tiêu cơ bản của an toàn thông tin

+ Đảm bảo tính sẵn sàng (**Availability**)

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 99,99%

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Mục tiêu cơ bản của an toàn thông tin

+ Đảm bảo tính xác thực (**Authenticity**)

Đảm bảo rằng thông tin: giao dịch, hoặc các tài liệu (tài liệu điện tử hoặc tài liệu cứng) đều là thật, hay xác nhận rằng các bên liên quan biết họ là ai trong hệ thống.

+ Đảm bảo tính không thể chối cãi (**Non repudiation**)

Không thể chối cãi có nghĩa rằng trong quá trình giao dịch trên mạng, một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác. Ví dụ: giao dịch mua hàng qua mạng.

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Tình hình an ninh mạng tại Việt Nam.

- Từ 2010 đến 2019 đã có 53.744 lượt cổng thông tin, trang tin điện tử có tên miền .vn bị tấn công
- Từ 2001 - 2019, phát hiện hơn 1.100 vụ lộ, mất bí mật nhà nước, chủ yếu qua hệ thống thông tin
- Trong 2019, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới gần 1 tỷ USD, hơn 1,8 triệu máy tính bị mất dữ liệu do sự lan tràn của các loại mã độc mã hóa dữ liệu tống tiền (***ransomware***), trong đó có nhiều máy chủ chứa dữ liệu của các cơ quan, gây đình trệ hoạt động của nhiều cơ quan, doanh nghiệp (***theo BKAV-2019***)

Tham khảo:

(1). Lê Văn Thắng (2019), "An ninh thông tin của Việt Nam trong điều kiện hiện nay: Thực trạng, vấn đề đặt ra và giải pháp", Đề tài khoa học cấp Nhà nước, Hà Nội.
(2). Tập đoàn BKAV (2019), Báo cáo tổng kết công tác an ninh mạng năm 2019.

Chuyển đổi số và cuộc cách mạng công nghiệp 4.0 tại Việt Nam.

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Sự cần thiết của an toàn thông tin

Hệ thống thông tin là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, là tài sản quan trọng nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu và rủi do.

Do máy tính được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng, các phiên bản được phát hành liên tục với các tính năng mới được thêm vào ngày càng nhiều, điều này làm cho các phần mềm không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống mạng, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các nguy cơ mất an toàn thông tin

Các giải pháp bảo vệ an toàn thông tin

Một số kỹ thuật an toàn và bảo mật thông tin

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các nguy cơ mất an toàn thông tin

+ Khía cạnh vật lý

+ Khía cạnh kĩ thuật

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các nguy cơ mất an toàn thông tin

Khía cạnh vật lý

Nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng, các phần tử phá hoại như nhân viên xấu bên trong và kẻ trộm bên ngoài.

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các nguy cơ mất an toàn thông tin

+ Khía cạnh kĩ thuật

- Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin: Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin. Kẻ xấu có thể sử dụng công cụ hoặc kỹ thuật của mình để thay đổi nội dung thông tin (các file) nhằm sai lệnh thông tin của chủ sở hữu hợp pháp.

- Nguy cơ bị tấn công bởi các phần mềm độc hại Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: **Virus**, sâu máy tính (**Worm**), phần mềm gián điệp (**Spyware**),...

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các nguy cơ mất an toàn thông tin

+ Khía cạnh kĩ thuật

- ✓ **Virus**: là một chương trình máy tính có thể tự sao chép chính nó lên những đĩa, file khác mà người sữ dụng không hay biết. Thông thường virus máy tính mang tính chất phá hoại, nó sẽ gây ra lỗi thi hành, lệch lạc hay hủy dữ liệu.

- ✓ **Worm**: Loại virus lây từ máy tính này sang máy tính khác qua mạng, khác với loại virus truyền thống trước đây chỉ lây trong nội bộ một máy tính và nó chỉ lây sang máy khác khi ai đó đem chương trình nhiễm virus sang máy này.

- ✓ **Trojan, Spyware, Adware**: Là những phần mềm gián điệp, chúng không lây lan như virus. Thường bằng cách nào đó (lừa đảo người sử dụng thông qua một trang web, hoặc một người cố tình gửi nó cho người khác) cài đặt và nằm vùng tại máy của nạn nhân, từ đó chúng gửi các thông tin lấy được ra bên ngoài hoặc hiện lên các quảng cáo ngoài ý muốn của nạn nhân.

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các nguy cơ mất an toàn thông tin

+ Khía cạnh kĩ thuật

- Nguy cơ xâm nhập từ lỗ hổng bảo mật: thường là do lỗi lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính. Hiện, nay các lỗ hổng bảo mật được phát hiện ngày càng nhiều trong các hệ điều hành, các web server hay các phần mềm khác.

- Nguy cơ xâm nhập do bị tấn công bằng cách phá mật khẩu: Quá trình truy cập vào một hệ điều hành có thể được bảo vệ bằng một khoản mục người dùng và một mật khẩu. Đôi khi người dùng khoản mục lại làm mất đi mục đích bảo vệ của nó bằng cách chia sẻ mật khẩu với những người khác, ghi mật khẩu ra và để nó công khai hoặc để ở một nơi nào đó cho dễ tìm trong khu vực làm việc của mình

- Nguy cơ mất an toàn thông tin do sử dụng e-mail Tấn công có chủ đích bằng thư điện tử là tấn công bằng email giả mạo giống như email được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus. Cách thức tấn công này thường nhằm vào một cá nhân hay một tổ chức cụ thể. Thư điện tử đính kèm tập tin chứa virus được gửi từ kẻ mạo danh là một đồng nghiệp hoặc một đối tác nào đó. Người dùng bị tấn công bằng thư điên tử có thể bị đánh cắp mật khẩu hoặc bị lây nhiễm virus

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các giải pháp bảo vệ an toàn thông tin

Bảo vệ thông tin về mặt vật lý

- Thiết bị lưu điện, lặp đặt hệ thống điều hòa nhiệt độ và độ ẩm.
- Luôn sẵn sàng các thiết bị chữa cháy nổ, không đặt các hóa chất gần thệ thống.
- Thường xuyên sao lưu dữ liệu.
- Sử dụng các chính sách vận hành hệ thống đúng quy trình, an toàn và bảo mật.

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các giải pháp bảo vệ an toàn thông tin

Bảo vệ về mặt kĩ thuật:

- Cung cấp những hướng dẫn, những quy tắc, và những quy trình để thiết lập một môi trường thông tin an toàn.
- Đào tạo cho người dùng về các phần mềm phá hoại.
- Yêu cầu người dùng phải quét các thiết bị lưu trữ bằng các phần mềm quét virus trước khi sử dụng chúng.
- Thiết lập các chính sách để ngăn chặn người dùng tự cài đặt các phần mềm riêng của họ.
- Thiết lập các chính sách để giảm thiểu hoặc ngăn chặn người dùng tải về các tệp và yêu cầu người dùng phải quét virus đối với các tệp này.
- Tạo một vùng riêng để người dùng cách ly các tệp có nguồn gốc không rõ ràng để quét chúng trước khi sử dụng.
- Xây dựng chính sách giới hạn quyền để kiểm soát truy cập vào hệ thống
- Thường xuyên cài đặt các bản cập nhật (updates) bảo vệ hệ thống của mình

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các giải pháp bảo vệ an toàn thông tin

Bảo vệ thông tin trước nguy cơ tấn công bằng cách phá mật khẩu

- Sử dụng phương thức chứng thực tên truy cập và mật khẩu là phương pháp được dùng phổ biến đối với các hệ thống vì vậy xây dựng một chính sách sử dụng mật tốt sẽ đạt hiệu quả cao như: Tạo một quy tắc đặt mật khẩu riêng cho mình, không nên dùng lại mật khẩu đã sử dụng, tránh những mật khẩu dễ đoán như ngày sinh, tên người thân,… thường xuyên thay đổi mật khẩu đăng nhập hệ thống để tránh trường hợp người dùng vô tình làm lộ mật khẩu hoặc kẻ xấu cố tình lấy cắp mật khẩu.

- Sử dụng các ký tự mật khẩu có tính an toàn cao

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Các giải pháp bảo vệ an toàn thông tin

Bảo vệ thông tin do nguy cơ do sử dụng e-mail

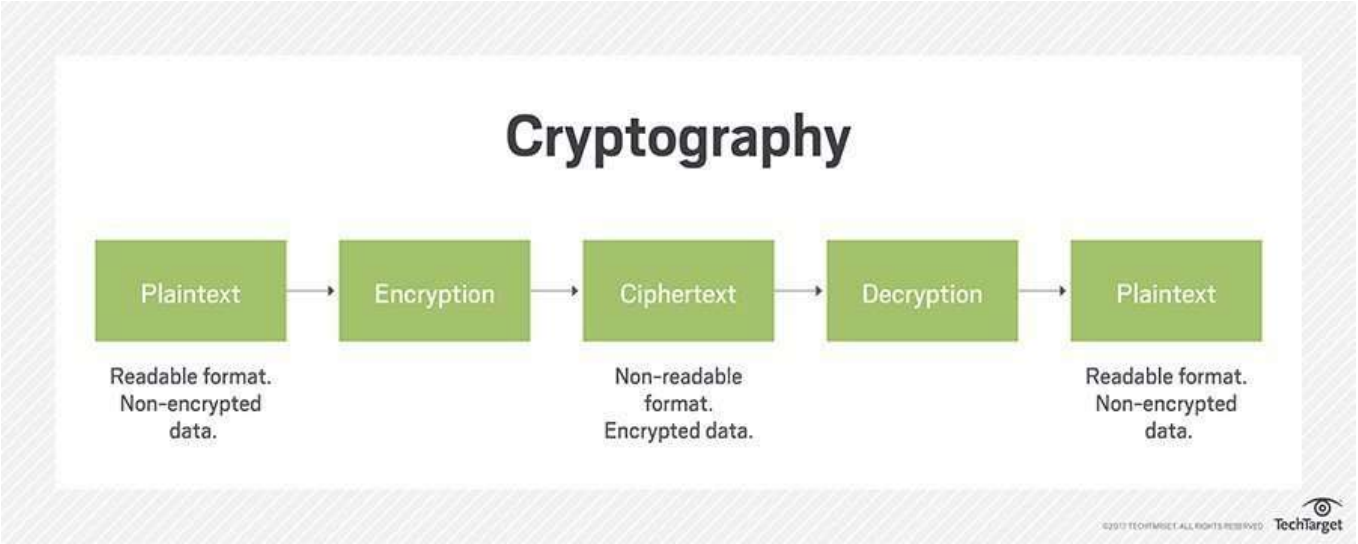
- Không mở bất kỳ tập tin đính kèm được gửi từ một địa chỉ e-mail mà không biết rõ hoặc không tin tưởng.
- Không mở bất kỳ e-mail nào mà mình cảm thấy nghi ngờ, thậm chí cả khi email này được gửi từ bạn bè hoặc đối tác bởi hầu hết virus được lan truyền qua đường e-mail và chúng sử dụng các địa chỉ trong sổ địa chỉ (Address Book) trong máy nạn nhân để tự phát tán. Do vậy, nếu không chắc chắn về một e-mail nào thì hãy tìm cách xác nhận lại từ phía người gửi.
- Không mở những tập tin đính kèm theo các e-mail có tiêu đề hấp dẫn, nhạy cảm; xóa các e-mail không rõ hoặc không mong muốn và không forward (chuyển tiếp) chúng cho bất kỳ ai hoặc reply (hồi âm) lại cho người gửi. Những e-mail này thường là thư rác (spam).

Các giải pháp bảo vệ an toàn thông tin

Bảo vệ thông tin do nguy cơ do sử dụng e-mail

- Không sao chép vào đĩa cứng bất kỳ tập tin nào mà bạn không biết rõ hoặc không tin tưởng về nguồn gốc xuất phát của nó.
- Thận trọng khi tải các tập tin từ Internet về đĩa cứng của máy tính. Dùng một chương trình diệt virus được cập nhật thường xuyên để kiểm tra những tập tin này. Nếu nghi ngờ về một tập tin chương trình hoặc một e-mail thì đừng bao giờ mở nó ra hoặc tải về máy tính của mình. Cách tốt nhất trong trường hợp này là xóa chúng hoặc không tải về máy tính của mình.
- Dùng một chương trình diệt virus tin cậy và được cập nhật thường xuyên như Norton Anti Virus, McAffee,... Sử dụng những chương trình diệt virus có thể chạy thường trú trong bộ nhớ để chúng thường xuyên giám sát các hoạt động trên máy tính và ở chức năng quét e-mail.

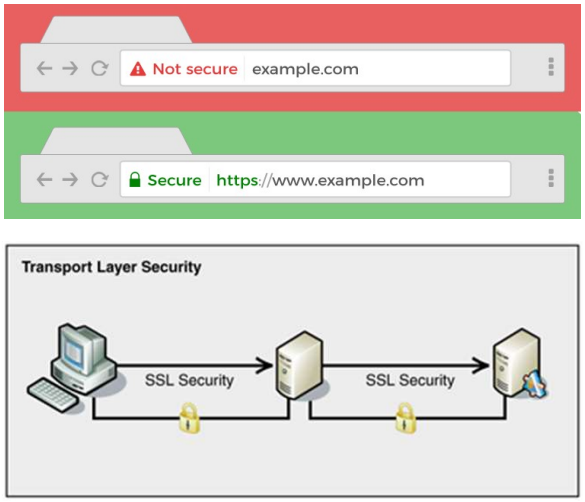
Mã hoá thông tin (Cryptography)



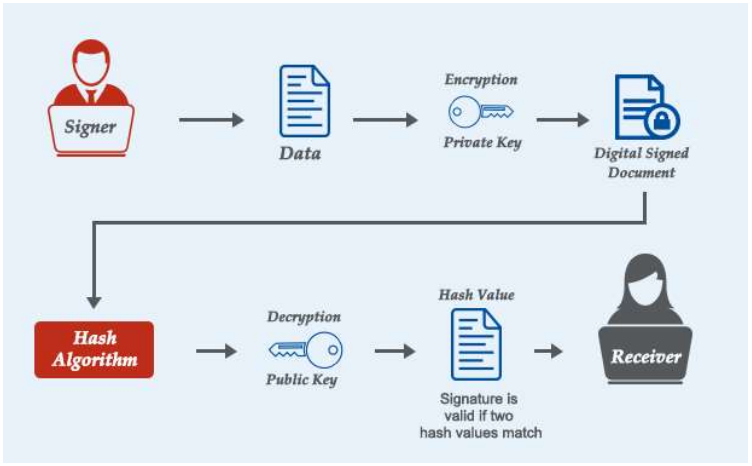
CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Mã hoá thông tin (Cryptohraphy)

Tại sao cần phải mã hoá thông tin?



Network security



Digital signature

Cryptocurrency or “digital money.”