**Họ Tên: Trịnh Xuân Chinh**

**LỚP: TH24.09**

**BÀI KIỂM TRA SỐ 1: HỌC PHẦN BẢO MẬT**

**(Thời gian làm bài 120 phút)**

Bài 1. Vai trò của an toàn thông tin và bảo mật thông tin

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên,…đều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của doanh nghiệp là những đòi hỏi ngày càng cao của môi trường kinh doanh yêu cầu doanh nghiệp cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua Internet hay Intranet. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng của công ty và quan hệ với khách hàng.

Vì vậy an toàn và bảo mật thông tin là sự bảo vệ thông tin và các hệ thống thông tin,tránh bị truy nhập,sử dụng , tiết lộ,gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm đảm bảo tính nguyên vẹn , tính bảo mật và tính khả dụng của thông tin.

Bảo mật thông tin là hoạt động duy trì tính bảo mật ,tính toàn vẹn và tính sẵn sàng cho toàn bộ thông tin . ba yêu tố này luôn đi cùng nhau và không thể tách rời.

+ Tính bảo mật : Đảm bảo mọi thông tin quan trọng không bị rò rỉ hay đánh cắp. thông tin chỉ được phép truy cập bởi những người được cấp phép

+ Tình toàn vẹn : Đảm bảo thông tin không bị thay đổi hoặc chỉ được phép chỉnh sửa bởi người có thẩm quyền . Ngoài ra tính toàn vẹn còn đảm bảo thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

An toàn và bảo vệ thông tin càng ngày càng có vai trò quan trọng trong cuộc sống tới cá nhân, tổ chức và chính phủ.

Bài 2: Trình bày mô hình mạng an toàn

Để giúp cho việc hoạch định chính sách và xây dựng hệ thống an ninh tốt. Bộ phận chuẩn hóa tiêu chuẩn của tổ chức truyền thông quốc tế (International Telecommunication Union) đã nghiên cứu và đề ra Kiến trúc an ninh X800 dành cho hệ thống trao đổi thông tin mở OSI. Trong đó định nghĩa một cách hệ thống phương pháp xác định và cung cấp các yêu cầu an toàn.Nó cung cấp cho chúng ta một cách nhìn tổng quát, hữu ích về các khái niệm mà chúng ta nghiên cứu.

Trước hết nói về dich vụ an toàn, X800 định nghĩa đây là dịch vụ cung cấp cho tầng giao thức của các hệ thống mở trao đổi thông tin, mà đảm bảo an toàn thông tin cần thiết cho hệ thống và cho việc truyền dữ liệu.

Trong tài liệu các thuật ngữ chuẩn trên Internet RFC 2828 đã nêu định nghĩa cụ thể hơn dich vụ an toàn là dịch vụ trao đổi và xử lý cung cấp cho hệ thống việc bảo vệ đặc biệt cho các thông tin nguồn.Tài liệu X800 đưa ra định nghĩa dịch vụ theo 5 loại chính:

- Xác thực: tin tưởng là thực thể trao đổi đúng là cái đã tuyên bố. Người đang trao đổi xưng tên với mình đúng là anh ta, không cho phép người khác mạo danh.

- Quyền truy cập: ngăn cấm việc sử dụng nguồn thông tin không đúng vai trò. Mỗi đối tượng trong hệ thống được cung cấp các quyền hạn nhất định và chỉ được hành động trong khuôn khổ các quyền hạn đó.

- Bảo mật dữ liệu: bảo vệ dữ liệu không bị khám phá bởi người không có quyền. Chẳng hạn như dùng các ký hiệu khác để thay thế các ký hiệu trong bản tin, mà chỉ người có bản quyền mới có thể khôi phục nguyên bản của nó.

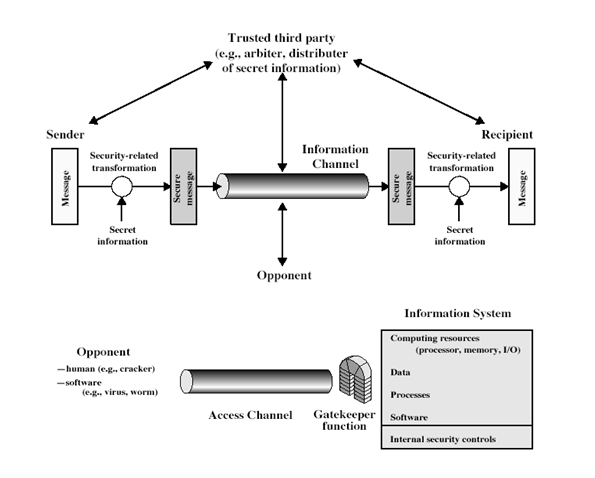
- Toàn vẹn dữ liệu: tin tưởng là dữ liệu được gửi từ người có quyền. Nếu có thay đổi như làm trì hoãn về mặt thời gian hay sửa đổi thông tin, thì xác thực sẽ cho cách kiểm tra nhận biết là có các hiện tượng đó đã xảy ra.

- Không từ chối: chống lại việc chối bỏ của một trong các bên tham gia trao đổi. Người gửi cũng không trối bỏ là mình đã gửi thông tin với nội dung như vậy và người nhận không thể nói dối là tôi chưa nhận được thông tin đó. Điều này là rất cần thiết trong việc trao đổi, thỏa thuận thông tin hàng ngày.

Cơ chế an toàn được định nghĩa trong X800 như sau:

- Cơ chế an toàn chuyên dụng được cài đặt trong một giao thức của một tầng vận chuyển nào đó: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, đệm truyền, kiểm soát định hướng, công chứng.

- Cơ chế an toàn phổ dụng không chỉ rõ được dùng cho giao thức trên tầng nào hoặc dịch vụ an ninh cụ thể nào: chức năng tin cậy cho một tiêu chuẩn nào đó, nhãn an toàn chứng tỏ đối tượng có tính chất nhất định, phát hiện sự kiện, vết theo dõi an toàn, khôi phục an toàn.



Bài 3: Hãy nêu cách suy đoán mật khẩu, đưa ra các giải pháp bảo vệ mật khẩu.

Đoán mật khẩu là một trong các hướng tấn công chung nhất. Kẻ tấn công đã biết tên người sử dụng đăng nhập (từ trang email/web) và tìm cách đoán mật khẩu.

* + Mặc định, mật khẩu ngắn, tìm kiếm các từ chung
  + Thông tin của người dùng (thay đổi tên, ngày sinh, số điện thoại, các mối quan tâm và từ chung)
  + Tìm kiếm tổng thể mọi khả năng của mật khẩu

Các giải pháp bảo vệ mật khẩu:

* + độ dài tối thiểu > 6
  + đòi hỏi trộn chữ hoa và chữ thường, số và dấu chấm
  + không chọn từ trong từ điển
  + Nhưng nên chọn sao cho nhiều người không để ý

Tạo mật khẩu – máy tính tự sinh

* + Cho máy tính tự tạo mật khẩu
  + Nếu ngẫu nhiên không dễ nhớ, thì sẽ viết xuống (hội chứng nhãn khó chịu)
  + Ngay cả phát âm được cũng không nhớ
  + Có câu chuyện về việc chấp nhận của người sử dụng tồi
  + FIPS PUB 181 là một trong những bộ sinh tốt nhất
    - Có cả mô tả và code ví dụ
    - Sinh từ việc ghép ngẫu nhiên các âm tiết phát âm được

Tạo mật khẩu - kiểm tra trước

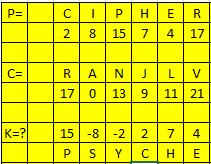
* + Cách tiếp cận hưá hẹn nhất để có thể cải thiện an toàn mật khẩu
  + Cho phép người sử dụng chọn trước mật khẩu của mình
  + Nhưng để cho hệ thống kiểm chứng xem nó có chấp nhận được không
    - Bắt buộc theo qui tắc đơn giản
    - So sánh với từ điển các mật khẩu tồi
    - Sử dụng mô hình thuật toán Markov hoặc bộ lọc để chống các cách chọn tồi

Bài 4: Cho *Hệ mã Vigenere*

Cho hệ mã Vigenere có M = 6. Giải mã xâu C = “RANJLV” người ta thu được bản rõ là “CIPHER”.



1. Tìm khóa đã sử dụng của hệ mã trên.



K = PSYCHE

1. Dùng khóa tìm được ở phần trên hãy hãy giải mã xâu M = “PLDKCI DUJQJO“.



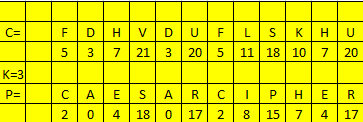
P = ATFIVE OCLOCK

Bài 5: Cho biến đọan mã sau dùng mã Ceasar

C: " FDHVDU FLSKHU"



1. Tìm bản rõ P=?



P = CAESAR CIPHER

1. Sử dụng k=9 . Mã hóa bản rõ sau P: “CACH MANG CONG NGHIEP”



C = LJLQ VJWP LXWP WPQRNY

Bài 6: Cho hệ mã Vigenere . Biết bản mã C: “FSP PPVNZCBXEWH” có bản rõ tương ứng P: “ Web Development” Hãy tìm khóa K ??



1. Hãy tìm khóa mã hóa đã dùng của hệ mã trên.



K = JOOMLA

1. Dùng khóa tìm được ở phần trên hãy giải mã bản mã C = “Ymoyxnx Fdwrkj mzr”.

P = Pyammno Rpkgka ylf

Bài 7: Sử dụng hệ mã hóa hàng rào. ( Trình bày rõ cách làm)

1. Mã hóa bản rõ sau: P: “Chúng tôi là những sinh viên CNTT HUBT” với K=4

C H P=C H N U T B T T

N U

T B

T T

1. Tìm bản rõ P của bản mã sau.

“ CGHHGNONEOINGTNI”

k=3

C G H H N G

O N E O T

N G T N I

Bài 8: Sử dụng hệ mã hóa Playfair mã hóa từ khóa K sau:

K= “PlayFair Cipher”

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | L | A | Y | F |
| I | R | C | H | E |
| B | D | G | K | M |
| N | O | Q | S | T |
| U | V | W | X | Z |