Tổng quan

1. Các khái niệm

* Hệ thống thông tin: phần cứng + thông tin/dữ liệu + con người quản lý+ phần mềm+ các hoạt động xử lí
* ứng dụng: chương trình phần mềm phục vụ nhu cầu người dùng
* an toàn: trạng thái được bảo vệ trước các rủi ro khách/chủ quan
* an toàn tt: bảo vệ tt trước rủi ro
* bảo mật: bảo vệ 2 thuộc tính: tính toàn vẹn + bí mật dữ liệu/tt
* an ninh: đảm bảo an toàn cho các thực thể trước các mối đe dọa
* an ninh mạng: đảm bảo an toàn cho hệ thống mạng máy tính khỏi các mối đe dọa
* dữ liệu: các giá trị của tt định lượng hoặc đính tính của các sự vật, hiện tượng trong cs. Được lưu trữ để xử lý
* thông tin: là dữ liệu đã được xử lý, phân tích, tổ chức nhằm để hiểu rõ hơn sự vật, sự việc, hiện tượng theo 1 góc độ nhất định.
* Yêu cầu bảo mật hệ thống tt: đảm bảo 🡺 tính toàn vẹn + bí mật + tính sẵn sàng + chống chối bỏ (thông tin nơi gửi/nhận, sao kê, hóa đơn thanh toán….)

1. Xác định các mối nguy hiểm:

* Xđ mối đe dọa:

+ mối đe dọa bảo mật: những sk có ảnh hưởng đến an toàn hệ thống tt

+ mối đe dọa có 4 loại: ---xem tt bất hợp pháp

--- chỉnh sửa tt bất hợp pháp

--- từ chối dịch vụ

--- từ chối hành vi

* Các mối đe dọa thường gặp:

+ lỗi và thiếu sót của user

+ gian lận và đánh cắp tt

+ kẻ tấn công nguy hiểm

+ mã nguy hiểm

+ tấn công từ chối dịch vụ

+ social engineering

* Lỗi và thiếu sót của user:

+ mối đe dọa hthong tt xuất phát từ những lỗi bảo mật, lỗi thao tác của những user trong hệ thống

+ là mối đe dọa hàng đầu đối với 1 hệ thống tt

+ giải pháp:

* Huấn luyện user thực hiện đúng thao tác, hạn chế sai sót
* Nguyên tắc: quyền tối thiểu
* Thường xuyên back-up hệ thống
* Tấn công mạng:

+ kẻ tấn công nguy hiểm xâm nhập vào hệ thống để tìm kiếm tt, phá hoại dữ liệu, phá hủy hệ thống

+ 5 bước để tấn công vào 1 hệ thống:

* Thăm dò
* Quét lỗ hổng để tấn công
* Cố gắng lấy quyền truy cập
* Duy trì kết nối
* Xóa dấu vết
* Mã độc:

+ là 1 đoạn mã không mong muốn được nhúng trong 1 program nhằm thực hiện các truy cập trái phép vào hệ thống mt để thu thập các tt nhạy cảm, làm gián đoạn hđ or gây hại cho hthong mt

* Tấn công từ chối dịch vụ:

+ là kiểu tấn công ngăn không cho những user khác truy cập vào hệ thống

+ làm cho hthong bị quá tải và k thể hđ

+ DoS: tấn công one – to – one

+ DdoS:

* Sd các Zombie host
* Tấn công many-to-one
* Social engineering:

+ sd sự ảnh hưởng và thuyết phục để đánh lừa user nhằm khai thác tt

* Điều khiển truy cập:
* Là cơ chế điều khiển, qli các truy cập vào hệ thống csdl
* Các bước ddkhien truy cập:

+ định danh: user cung cấp danh định

+ xác thực: user chứng minh định danh là đúng

+ ủy quyền: xđ quyền mà user có

* Cơ chế xd các tập luật điều khiển truy cập: cách thức để xét 1 truy cập là cho phép or bị từ chối

+ dkhien truy cập tùy quyền

+ dkhien truy cập bắt buộc

1. 1 số thuật ngữ

* Mật mã học: ngành KH nghiên cứu các kĩ thuật toán học => cung cấp dịch vụ bảo vệ tt
* Hệ mật mã: tập hợp các thuật toán, các thủ tục kết hợp => che dấu tt và làm rõ nó
* Mã hóa: quá trình chuyển tt có thể đọc (bản rõ) thành tt không thể đọc (bản mã)
* Giải mã: quá trình ngược lại với mã hóa
* Thuật toán mã hóa: các thủ tục tính toán => che dấu và làm rõ tt
* 1 khóa: 1 gtri làm cho thuật toán mã hóa chạy theo cách riêng biệt => sinh ra bản rõ riêng biệt tùy theo khóa. Khóa càng lớn => bản mã kq càng an toàn. Kích thước mã đo bằng bit. Phạm vi các gtri có thể có => không gian khóa
* Phân tích mã: quá trình or nghệ thuật ptich hệ mật mã or ktra tính toàn vẹn của nó or phá nó vì lí do bí mật
* Kẻ tấn công: =)))
  1. Định nghĩa hệ mật mã

// P: bản rõ

// C: bản mã

// K: khóa

// E: các quy tắc mã hóa

// D: các quy tắc giải mã

🡺 1 hệ mật: là 1 bộ 5 thành phần: P, C, K, E, D thỏa mãn các dkien:

……………………………………

……………………………………

* Mã hóa đối xứng: mã hóa và giải mã dùng cùng 1 khóa
* Hạn chế: không an toàn vì gửi bản mã & khóa trên cùng 1 đường truyền/kênh => có thể bị giải mã
* Khắc phục: gửi bản mã và khóa trên các kênh/ phương thức khác nhau
* Kết luận: vẫn không quá tối ưu
* Mã hóa bất đối xứng:

+ người gửi : gửi bản mã ( dùng public key của người nhận để mã hóa) cho ng nhận

+ người nhận: giải mã bản mã nhận được bằng private key của mình

* Ưu điểm: an toàn tt
  1. ………………..

1. Cơ sở tóan học