Chương 1: Tổng quan về an toàn bảo mật hệ thống thông tin

26. Tại sao cần phải đảm bảo an toàn thông tin ?

A. Có quá nhiều thiết bị kết nối mạng với nhiều nguy cơ đe doạ (7 - 8 slide)

B. Có quá nhiều phần mềm độc hại

C. Có quá nhiều nguy cơ tấn công

D. Có quá nhiều thiết bị kết nối mạng

26. Các mối nguy cơ và đe doạ thường trực là:

A. Tin tặc và các phần mềm độc hại (18 slide)

B. Mất thông tin và các phần mềm nghe lén

C. Phần cứng và phần mềm độc hại

D. Các phần mềm độc hại

26. Hệ thống thông tin là:

A. Một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số (19 slide)

B. Một hệ thống gồm các thành phần phần cứng và phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin

C. Một hệ thống gồm các thành phần phần cứng nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

D. Một hệ thống gồm các thành phần phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

5. Người sử dụng **hệ thống thông tin quản lý** trong mô hình 4 loại hệ thống thông tin là:

A. Quản lý cao cấp

B. Giám đốc điều hành

C. Nhân viên

D. Quản lý bộ phận (21 slide)

5. Người sử dụng **hệ thống trợ giúp ra quyết định** trong mô hình 4 loại hệ thống thông tin là:

A. Nhân viên

B. Quản lý bộ phận

C. Quản lý cao cấp (21 slide)

D. Giám đốc điều hành

5. Các thành phần của hệ thống thông tin dựa trên máy tính là:

A. Phần cứng (Hardware), phần mềm (Software), cơ sở dữ liệu (Databases), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures) (24 slide)

B. Phần cứng (Hardware), phần mềm (Software), người dùng (Actor), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures)

C. Phần cứng (Hardware), phần mềm (Software), dữ liệu (Data), bảo vệ (Security), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures)

D. Phần cứng (Hardware), phần mềm (Software), cơ sở dữ liệu (Databases), mạng riêng ảo (VPN), tập các lệnh kết hợp (Procedures)

10. An toàn thông tin (Information Security) là gì?

A. Là việc phòng chống đánh cắp thông tin

B. Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép (25 slide)

C. Là việc bảo vệ chống sử dụng, tiết lộ, sửa đổi, vận chuyển hoặc phá hủy thông tin một cách trái phép

D. Là việc phòng chống tấn công mạng

2. An toàn thông tin gồm hai lĩnh vực chính là:

A. An ninh mạng và An toàn hệ thống

B. An toàn máy tính và An toàn Internet

C. An toàn máy tính và An ninh mạng

D. An toàn công nghệ thông tin và Đảm bảo thông tin (25 slide)

30. Đảm bảo thông tin (Information assurance) thường được thực hiện bằng cách:

A. Sử dụng kỹ thuật tạo dự phòng ra đĩa cứng

B. Sử dụng kỹ thuật tạo dự phòng ra băng từ

C. Sử dụng kỹ thuật tạo dự phòng ngoại vi (25 slide)

D. Sử dụng kỹ thuật tạo dự phòng cục bộ

22. Các thành phần chính của an toàn thông tin gồm:

A. An toàn máy tính, An ninh mạng, Chính sách ATTT

B. An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT (26 slide)

C. An toàn dữ liệu, Quản lý ATTT và Chính sách ATTT

D. An toàn máy tính, An ninh mạng, Quản lý ATTT

22. Nội dung của an toàn máy tính và dữ liệu bao gồm:

A. Đảm bảo an toàn hệ điều hành, ứng dụng, dịch vụ.

B. Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố.

C. Vấn đề phòng chống phần mềm độc hại

D. Tất cả các đáp án trên (13 gt)

21. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm:

A. VPN, SSL/TLS, PGP

B. Điều khiển truy nhập

C. Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã (13 gt)

D. Tường lửa, proxy

7. Một trong các nội dung rất quan trọng của quản lý an toàn thông tin là:

A. Quản lý các ứng dụng

B. Quản lý hệ thống

C. Quản lý hệ điều hành

D. Quản lý rủi ro (14 gt)

25. Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do

A. Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian (14 gt)

B. Trình độ cao của tin tặc và công cụ tấn công ngày càng phổ biến

C. Số lượng và khả năng phá hoại của các phần mềm độc hại ngày càng tăng

D. Máy tính, hệ điều hành và các phần mềm được nâng cấp nhanh chóng

25. Chính sách an toàn thông tin không bao gồm:

A. Chính sách an toàn mức người dùng (14 gt)

B. Chính sách an toàn ở mức vật lý

C. Chính sách an toàn ở mức tổ chức

D. Chính sách an toàn ở mức logic

4. An toàn hệ thống thông tin là:

A. Việc đảm bảo thông tin trong hệ thống không bị đánh cắp

B. Việc đảm bảo cho hệ thống thông tin hoạt động trơn tru, ổn định

C. Việc đảm bảo cho hệ thống thông tin không bị tấn công

D. Việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin (28 slide)

24. Các yêu cầu cơ bản trong đảm bảo an toàn thông tin và an toàn hệ thống thông tin gồm:

A. Bảo mật, Toàn vẹn và Khả dụng

B. Bảo mật, Toàn vẹn và Sẵn dùng

C. Bí mật, Toàn vẹn và Sẵn dùng (28 slide)

D. Bí mật, Toàn vẹn và không chối bỏ

28. Tính bí mật của thông tin có thể được đảm bảo bằng:

A. Bảo vệ vật lý

B. Các kỹ thuật mã hóa

C. sử dụng VPN

D. Bảo vệ vật lý, VPN, hoặc mã hóa (16 gt)

8. Một thông điệp có nội dung nhạy cảm truyền trên mạng bị sửa đổi. Các thuộc tính an toàn thông tin nào bị vi phạm?

A. Bí mật, Toàn vẹn và sẵn dùng

B. Bí mật và Toàn vẹn (30 slide)

C. Bí mật

D. Toàn vẹn

9. Trong các vùng hạ tầng CNTT, vùng nào có nhiều mối đe dọa nguy cơ nhất?

A. Vùng máy trạm

B. Vùng người dùng (19 gt)

C. Vùng mạng LAN-to-WAN

D. Vùng mạng LAN

9. Tính toàn vẹn liên quan đến …….. và …….. của dữ liệu.

A. Tính hợp lệ, sự nghiêm ngặt

B. Tính hợp lệ, sự chính xác (32 slide)

C. Sự hợp pháp, sự chính xác

D. Sự hợp pháp, sự nghiêm ngặt

9. Thông tin hoặc dữ liệu là toàn vẹn nếu nó thỏa mãn điều kiện:

A. Không bị thay đổi

B. Hợp lệ

C. Chính xác

D. Cả 3 đáp án trên (32 slide)

9. Công thức tính tỷ lệ phục vụ của tính sẵn dùng là:

A. A = (UPtime)/(Loadtime + DownTime)

B. A = (UPtime)/(Uptime + DownTime) (34 slide)

C. A = (UPtime)/(Loadtime + DownTime + Uptime)

D. A = (UPtime)/(Loadtime + UpTime)

9. Các đe dọa với tầng người dùng bao gồm:

A. Coi nhẹ và vi phạm các chính sách an toàn, đưa các công cụ lưu trữ cá nhân vào hệ thống, thiếu ý thức về vấn đề an ninh an toàn (38 slide)

B. Coi nhẹ chính sách an toàn và thăm dò rà soát trái phép các cổng dịch vụ, thiếu ý thức về vấn đề an ninh an toàn

C. Đưa các công cụ lưu trữ file cá nhân vào hệ thống và truy nhập trái phép vào máy trạm

D. Đưa các công cụ lưu trữ file cá nhân vào hệ thống và nguy cơ từ người dùng giả mạo trong mạng WAN

9. Các đe dọa với vùng máy trạm bao gồm:

A. Coi nhẹ và vi phạm các chính sách an toàn, đưa các công cụ lưu trữ file cá nhân vào hệ thống, thiếu ý thức về vấn đề an ninh an toàn

B. Coi nhẹ và vi phạm các chính sách an toàn, thăm dò rà soát trái phép các cổng dịch vụ, thiếu ý thức về vấn đề an ninh an toàn

C. Đưa các công cụ lưu trữ file cá nhân vào hệ thống và truy nhập trái phép vào máy trạm (39 slide)

D. Đưa các công cụ lưu trữ file cá nhân vào hệ thống và nguy cơ từ người dùng giả mạo trong mạng WAN

9. Các lỗ hổng an ninh trong hệ điều hành máy chủ là mối đe dọa thuộc vùng nào trong 7 vùng cơ sở hạ tầng CNTT ?

A. Vùng máy trạm

B. Vùng mạng WAN

C. Vùng mạng LAN-to-WAN

D. Vùng mạng LAN (40 slide)

9. Nguy cơ bị tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS) thường gặp ở vùng nào trong 7 vùng cơ sở hạ tầng CNTT?

A. Vùng máy trạm

B. Vùng mạng WAN (42 slide)

C. Vùng mạng LAN-to-WAN

D. Vùng mạng LAN

9. Trong các vùng hạ tầng CNTT vùng nào dễ bị tấn công kiểu vét cạn?

A. Vùng người dùng

B. Vùng truy cập từ xa (43 slide)

C. Vùng mạng LAN-to-WAN

D. Vùng hệ thống ứng dụng

9. Trong các vùng hạ tầng CNTT, vùng nào có lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ ?

A. Vùng máy trạm

B. Vùng mạng LAN-to-WAN

C. Vùng truy nhập từ xa

D. Vùng hệ thống/ ứng dụng (44 slide)

6. Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là:

A. Phòng vệ nhiều lớp có chiều sâu (45 slide)

B. Cần đầu tư trang thiết bị và chuyên gia đảm bảo an toàn

C. Cần mua sắm và lắp đặt nhiều thiết bị an ninh chuyên dụng

D. Cân bằng giữa tính hữu dụng, chi phí và tính năng

6. Việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống cần thực hiện theo nguyên tắc chung là:

A. Cân bằng giữa an toàn, hữu dụng và chi phí (46 slide)

B. Cân bằng giữa an toàn, hữu dụng và tin cậy

C. Cân bằng giữa an toàn, chi phí và chất lượng

D. Cân bằng giữa an toàn, chi phí và tin cậy

1. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin thường gồm các lớp:

A. An ninh tổ chức, An ninh mạng và Điều khiển truy cập

B. An ninh tổ chức, Tưởng lửa và Điều khiển truy cập

C. An ninh tổ chức, An ninh mạng và An toàn hệ điều hành và ứng dụng

D. An ninh tổ chức, An ninh mạng và An ninh hệ thống (51 slide)

33. Đáp án nào chỉ gồm các lớp con của lớp phòng vệ an ninh mạng ?

A. Lớp chính sách và thủ tục đảm bảo an toàn thông tin; Lớp bảo vệ vật lý

B. Lớp bảo vệ vùng hạn chế truy nhập; Lớp các tường lửa, mạng riêng ảo (21 gt)

C. Lớp phát hiện và ngăn chặn phần mềm độc hại; Lớp các tường lửa, mạng riêng ảo

D. Lớp quản trị tài khoản và phân quyền người dùng; Lớp tăng cường an ninh hệ thống

33. Quản lý các bản vá và cập nhật phần mềm là phần việc thuộc lớp bảo vệ nào trong mô hình tổng thể đảm bảo an toàn hệ thống thông tin?

A. Lớp an ninh mạng

B. Lớp an ninh hệ thống (51 slide)

C. Lớp an ninh cơ quan/tổ chức

D. Lớp an ninh hệ điều hành và phần mềm

Chương 2: Các dạng tấn công và phần mềm độc hại

11. Tìm phát biểu đúng trong các phát biểu sau:

A. Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống mạng.

B. Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (3 slide)

C. Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính.

D. Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính và mạng.

17. Điểm yếu là:

A. Một lỗi khi xây dựng phần cứng máy tính

B. Một lỗi hoặc một khiếm khuyết tồn tại trên hệ thống (3 slide)

C. Là một khiếm khuyết của phần mềm

D. Một lỗi hoặc một khiếm khuyết tồn tại trong kết nối mạng

17. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do:

A. Lỗi thiết kế, lỗi cài đặt và lập trình

B. Tất cả các khâu trong quá trình phát triển và vận hành (23 gt)

C. Lỗi quản trị

D. Lỗi cấu hình hoạt động

14. Tìm phát biểu đúng trong các phát biểu sau:

A. Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần mềm

B. Điểm yếu chỉ xuất hiện khi hệ thống bị tấn công

C. Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm (23 gt)

D. Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần cứng

29. Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc:

A. Khai thác nhằm đánh cắp các thông tin trong hệ thống

B. Khai thác, gây tổn hại đến các thuộc tính an ninh của hệ thống đó (23 gt)

C. Khai thác, tấn công phá hoại và gây tê liệt hệ thống

D. Khai thác nhằm chiếm quyền điều khiển hệ thống

29. Tìm phát biểu đúng:

A. Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép hacker có thể gây hại

B. Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây hại (3 slide)

C. Lỗ hổng là bất kỳ điểm yếu nào trong mạng cho phép mối đe dọa có thể gây hại

D. Lỗ hổng là bất kỳ điều gì trong hệ thống cho phép mối đe dọa có thể gây hại

20. Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống:

A. Hệ điều hành

B. Các dịch vụ mạng

C. Các ứng dụng (23 gt)

D. Các thành phần phần cứng

20. Các mức độ nghiêm trọng của các lỗ hổng bảo mật theo Microsoft là:

A. Nguy hiểm, Cao, Trung bình, Thấp

B. Quan trọng, Cao, Trung bình, Thấp

C. Nguy hiểm, Quan trọng, Trung bình, Thấp (23 gt)

D. Cao, Quan trọng, Trung bình, Không quan trọng

11. Đâu không phải là mối quan hệ giữa mối đe doạ và lỗ hổng:

A. Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại

B. Không thể triệt tiêu được hết các lỗ hổng, nhưng có thể giảm thiểu các mối đe dọa, qua đó giảm thiểu khả năng bị tận dụng để tấn công (5 slide)

C. Nếu tồn tại một lỗ hổng trong hệ thống sẽ có khả năng một mối đe dọa thành hiện thực

D. Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công

18. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể...

A. Triệt tiêu được hết các nguy cơ

B. Triệt tiêu được hết các mối đe dọa

C. Giảm thiểu các lỗ hổng bảo mật (5 slide)

D. Kiểm soát chặt chẽ người dùng

54. Một trong các mối đe dọa an toàn thông tin thường gặp là:

A. Phần mềm nghe lén

B. Phần mềm quảng cáo

C. Phần mềm phá mã

D. Phần mềm độc hại (6 slide)

54. Các lỗ hổng tồn tại phổ biến trong hệ điều hành và các phần mềm ứng dụng là:

A. Lỗi tràn bộ đệm và cấu hình

B. Lỗi cài đặt và quản trị

C. Lỗi cài đặt và cấu hình

D. Lỗi tràn bộ đệm và lỗi không kiểm tra đầu vào (8 slide)

41. Dạng tấn công giả mạo thông tin thường để đánh lừa người dùng thông thường là:

A. Modifications

B. Fabrications (9 slide)

C. Interruptions

D. Interceptions

38. Dạng tấn công chặn bắt thông tin truyền trên mạng để **sửa đổi** hoặc lạm dụng là:

A. Fabrications

B. Modifications

C. Interruptions

D. Interceptions (9 slide)

36. Dạng tấn công gây ngắt quãng dịch vụ hoặc kênh truyền thông cho người dùng bình thường là:

A. Interceptions

B. Fabrications

C. Interruptions (9 slide)

D. Modifications

36. Dạng tấn công liên quan đến việc nghe trộm trên đường truyền và chuyển hướng thông tin để sử dụng trái phép là:

A. Interceptions (9 slide)

B. Fabrications

C. Interruptions

D. Modifications

37. Tấn công nghe lén là kiểu tấn công:

A. Thụ động (10 slide)

B. Chủ động

C. Chiếm quyền điều khiển

D. Chủ động và bị động

37. Công cụ Vulnerability scanners cho phép tin tặc:

A. Quét để tìm các cổng dịch vụ đang mở trên hệ thống

B. Thu thập các thông tin về các điểm yếu/lỗ hổng đã biết của hệ thống máy tính hoặc mạng (12 slide)

C. Nghe trộm và bắt các gói tin khi chúng được truyền trên mạng

D. Chặn bắt và sửa đổi thông tin

49. Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đánh cắp mật khẩu của người dùng bằng cách:

A. Tìm mật khẩu trong từ điển các mật khẩu

B. Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển (22 slide)

C. Vét cạn các mật khẩu có thể có

D. Lắng nghe trên đường truyền để đánh cắp mật khẩu

53. Mật khẩu an toàn trong thời điểm hiện tại là mật khẩu có:

A. Chứa các ký tự từ nhiều dạng ký tự

B. Khả năng chống tấn công phát lại và chứa các ký tự từ nhiều dạng ký tự

C. Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt (23 slide)

D. Độ dài lớn hơn hoặc bằng 8 ký tự

53. Tấn công bằng mã độc bao gồm các dạng tấn công:

A. Lợi dụng các lỗ hổng an ninh để chèn và thực hiện mã độc trên hệ thống nạn nhân

B. Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại

C. Lợi dụng các lỗ hổng an ninh để đánh cắp thông tin nhạy cảm

D. Cả A và B (24 slide)

53. Tấn công bằng mã độc có thể gồm:

A. Chèn mã XSS, CSRF

B. Chèn mã SQL

C. Tràn bộ đệm

D. Tất cả các đáp án trên (24 slide)

32. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng?

A. Lỗi tràn bộ đệm (31 gt)

B. Lỗi quản trị

C. Lỗi cấu hình

D. Lỗi thiết kế

31. Lỗi tràn bộ đệm là lỗi trong khâu:

A. Kiểm thử phần mềm

B. Thiết kế phần mềm

C. Lập trình phần mềm (31 gt)

D. Quản trị phần mềm

15. Tác hại của lỗi tràn bộ đệm:

A. Khiến ứng dụng ngừng hoạt động

B. Gây mất dữ liệu

C. Bị chiếm quyền kiểm soát hệ thống

D. Tất cả các đáp án trên (26 slide)

15. Các vùng bộ nhớ thường bị tràn gồm:

A. Ngăn xếp (Stack) và vùng nhớ cấp phát động (Heap) (27 slide)

B. Ngăn xếp (Stack) và Bộ nhớ đệm (Cache)

C. Hàng đợi (Queue) và vùng nhớ cấp phát động (Heap)

D. Hàng đợi (Queue) và Ngăn xếp (Stack)

34. Khi khai thác lỗi tràn bộ đệm, tin tặc thường chèn mã độc, gây tràn và ghi đè để sửa đổi thành phần nào sau đây của bộ nhớ Ngăn xếp để chuyển hướng nhằm thực hiện mã độc của mình:

A. Các biến đầu vào của hàm

B. Bộ đệm hoặc biến cục bộ của hàm

C. Con trỏ khung ngăn xếp (sfp)

D. Địa chỉ trở về của hàm (34 gt)

23. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode. Shellcode đó là dạng:

A. Mã Java

B. Mã C/C++

C. Mã máy (34 gt)

D. Mã Hợp ngữ

13. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng một số lệnh NOP (No Operation) ở phần đầu của mã tấn công. Mục đích của việc này là để:

A. Tăng khả năng phá hoại của mã tấn công

B. Tăng khả năng gây tràn bộ đệm

C. Tăng khả năng mã tấn công được thực hiện (35 gt)

D. Tăng khả năng gây lỗi chương trình

19. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị cơ sở dữ liệu:

A. SQL Server 2012

B. SQL Server 2000 (36 gt)

C. SQL Server 2008

D. SQL Server 2003

12. Đâu là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm?

A. Sử dụng tường lửa

B. Sử dụng công nghệ xác thực mạnh

C. Sử dụng các kỹ thuật mật mã

D. Sử dụng cơ chế cấm thực hiện mã trong dữ liệu (29 slide)

12. Biện pháp nào không thể phòng chống hiệu quả tấn công khai thác lỗi tràn bộ đệm ?

A. Sử dụng các thư viện an toàn hoặc ngôn ngữ lập trình không gây tràn

B. Đặt cơ chế không cho phép thự hiện mã trong dữ liệu (DEP)

C. Kiểm tra mã nguồn để tìm điểm có khả năng gây tràn và khắc phục

D. Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành (29 slide)

55. Dạng tấn công chèn mã nào được tin tặc sử dụng phổ biến trên các trang web nhắm đến các cơ sở dữ liệu ?

A. Tấn công chèn mã CSRF

B. Tấn công chèn mã XSS

C. Tấn công chèn mã HTML

D. Tấn công chèn mã SQL (33 slide)

55. Nguy cơ cao nhất mà một cuộc tấn công chèn mã SQL có thể gây ra cho một hệ thống là:

A. Đánh cắp các thông tin trong cơ sở dữ liệu

B. Chèn, xóa hoặc sửa đổi dữ liệu

C. Vượt qua các khâu xác thực người dùng

D. Chiếm quyền điều khiển hệ thống (33 slide)

59. Câu lệnh SQL nào tin tặc thường sử dụng trong tấn công chèn mã SQL để đánh cắp các thông tin trong cơ sở dữ liệu?

A. UNION INSERT

B. UNION SELECT (47 slide)

C. SELECT UNION

D. INSERT SELECT

59. Một trong các biện pháp hiệu quả phòng chống tấn công SQL Injection là:

A. Luôn kiểm tra và cập nhật các bản vá an ninh cho hệ điều hành và các phần mềm ứng dụng

B. Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy (54 slide)

C. Cấu hình máy chủ CSDL không cho thực thi lệnh từ xa

D. Không cho phép người dùng nhập mã vào các form

59. Tại sao việc sử dụng thủ tục cơ sở dữ liệu (Stored procedure) là một trong các biện pháp hiệu quả để ngăn chặn triệt để tấn công chèn mã SQL:

A. Thủ tục cơ sở dữ liệu có khả năng cấm chèn mã

B. Thủ tục cơ sở dữ liệu cho phép tách mã lệnh SQL khỏi dữ liệu người dùng (55 slide)

C. Thủ tục cơ sở dữ liệu độc lập với các ứng dụng

D. Thủ tục cơ sở dữ liệu lưu trong cơ sở dữ liệu và chạy nhanh hơn câu lệnh trực tiếp

59. Đâu không phải là một biện pháp phòng chống tấn công chèn mã SQL dựa trên thiết lập quyền người dùng phù hợp:

A. Không sử dụng người dùng có quyền system admin hoặc database owner làm người dùng truy cập dữ liệu

B. Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống (56 slide)

C. Chia nhóm người dùng, chỉ cấp quyền vừa đủ để truy cập các bảng biểu, thực hiện câu truy vấn và chạy các thủ tục

D. Tốt nhất, không cấp quyền thực hiện các câu truy vấn, cập nhật, sửa, xóa trực tiếp dữ liệu; Thủ tục hóa tất cả các câu lệnh và chỉ cấp quyền thực hiện thủ tục

45. Đâu là một công cụ kiểm tra lỗ hổng tấn công chèn mã SQL trên các website:

A. SQLCheck

B. SQL Server

C. SQLmap (57 slide)

D. SQLite

52. Tấn công từ chối dịch vụ (Dos - Denial of Service Attacks) là dạng tấn công có khả năng...

A. Gây hư hỏng phần cứng máy chủ

B. Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống (58 slide)

C. Đánh cắp dữ liệu trong hệ thống

D. Cản trở người dùng hợp pháp truy nhập các file dữ liệu của hệ thống

40. Trong tấn công DoS, việc gửi một lượng lớn các yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền là loại tấn công nào ?

A. Logic attacks

B. Passive attacks

C. Flooding attacks (58 slide)

D. Brute force attacks

40. Đâu là một kỹ thuật tấn công Dos?

A. UDP Ping

B. DNS Cache Poisoning

C. Smurf (58 slide)

D. DNS spoofing

37. Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào trong bộ giao thức TCP/IP?

A. Bắt tay 3 bước (44 gt)

B. Bắt tay 2 bước

C. Xác thực người dùng

D. Truyền dữ liệu

40. Một máy chủ trên mạng không chấp nhận các kết nối TCP nữa. Máy chủ thông báo rằng nó đã vượt quá giới hạn của phiên làm việc. Loại tấn công nào có thể đang xảy ra ?

A. Tấn công virus

B. Tấn công smurf

C. Tấn công TCP ACK (tấn công kiểu SYNACK) (59 slide)

D. TCP/IP hijacking

40. Trong quá trình thiết lập một phiên kết nối TCP (TCP three-way handshake) thứ tự các gói tin được gửi đi như thế nào?

A. SYN, URG, ACK

B. SYN, ACK, SYN-ACK

C. SYN, SYN-ACK, ACK (60 slide)

D. FIN, FIN-ACK, ACK

51. Đâu là một kỹ thuật tấn công Dos?

A. SYN requests

B. DNS spoofing

C. IP spoofing

D. Ping of death (44 gt)

67. Đâu là một biện pháp phòng chống SYN Floods:

A. SYN Firewalls

B. SYN IDS

C. SYN Proxy

D. SYN Cache (62 slide)

67. Đâu không phải là cách phòng chống SYN floods:

A. Sử dụng kỹ thuật lọc

B. Giảm thời gian chờ

C. Sử dụng firewall và proxy

D. Sử dụng mật khẩu mạnh (62 slide)

42. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và cơ chế gửi…

A. Unicast

B. Multicast

C. Anycast

D. Broadcast (63 slide)

42. Để thực hiện tấn công Smurf, tin tặc phải giả mạo địa chỉ gói tin ICMP trong yêu cầu tấn công. Tin tặc sử dụng:

A. Địa chỉ máy nạn nhân làm địa chỉ đích của gói tin

B. Địa chỉ của router làm địa chỉ đích của gói tin

C. Địa chỉ của router làm địa chỉ nguồn của gói tin

D. Địa chỉ máy nạn nhân làm địa chỉ nguồn của gói tin (63 slide)

42. Phát biểu nào sau đây mô tả đúng nhất về kỹ thuật tấn công Smurf:

A. Giả mạo địa chỉ IP nguồn trong gói tin ICMP là địa chỉ máy đích và chúng gửi đến tất cả các máy trong mạng

B. Giả mạo địa chỉ IP nguồn trong gói tin ICMP là địa chỉ quảng bá và chúng gửi đến máy đích

C. Tạo và gửi rất nhiều gói tin ICMP giả mạo có kích thước lớn đến máy đích

D. Giả mạo địa chỉ IP nguồn trong gói tin ICMP là địa chỉ máy đích và chúng gửi đến địa chỉ quảng bá của mạng (63 slide)

42. Các giao thức hay các dịch vụ nào sau đây nên loại bỏ trong mạng nếu có thể ?

A. Email

B. WWW

C. Telnet

D. ICMP (63 slide)

39. Có thể phòng chống tấn công Smurf bằng cách cấu hình các máy và router không trả lời...

A. Các yêu cầu ICMP hoặc các yêu cầu phát quảng bá (65 slide)

B. Các yêu cầu TCP hoặc các yêu cầu phát quảng bá

C. Các yêu cầu UPD hoặc các yêu cầu phát quảng bá

D. Các yêu cầu HTTP hoặc các yêu cầu phát quảng bá

46. Khác biệt cơ bản giữa tấn công DoS và DDoS là:

A. Phạm vi tấn công (số lượng host tham gia, 66 slide)

B. Mức độ gây hại

C. Kỹ thuật tấn công

D. Tần suất tấn công

43. Để thực hiện tấn công DDoS, tin tặc trước hết cần chiếm quyền điều khiển của một lượng lớn máy tính. Các máy tính bị chiếm quyền điều khiển thường được gọi là:

A. Zombies (68 slide)

B. Viruses

C. Worms

D. Trojans

43. Trong tấn công DDoS phản chiếu hay gián tiếp, có sự tham gia của một số lượng lớn máy chủ trên mạng Internet không bị tin tặc chiếm quyền điều khiển. Các máy chủ này được gọi là…

A. Reflectors (69 slide)

B. Injectors

C. Requesters

D. Forwarders

43. Điểm khác biệt giữa Reflective DDoS so với DDoS là gì ?

A. Một lượng lớn các yêu cầu kết nối giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân được gửi đến một số lớn các máy khác (69 slide)

B. Các máy tính do kẻ tấn công điều khiển (Staves/Zombies) trực tiếp tấn công máy nạn nhân

C. Tạo một lượng lớn yêu cầu kết nối giả mạo

D. Phạm vi tấn công lớn

47. Mục đích chính của tấn công giả mạo địa chỉ IP là:

A. Để vượt qua các hệ thống IPS và IDS

B. Để vượt qua các hàng rào kiểm soát an ninh (71 slide)

C. Để đánh cắp các dữ liệu nhạy cảm trên máy trạm

D. Để đánh cắp các dữ liệu nhạy cảm trên máy chủ

12. Nỗ lực tấn công để can thiệp vào một phiên liên lạc bằng việc thêm vào một máy tính giữa hai hệ thống được gọi là một:

A. TCP/IP hijacking

B. Tấn công cửa sau

C. Sâu

D. Tấn công dạng "Man in the middle" (77 slide)

56. Một trong các biện pháp có thể sử dụng để phòng chống tấn công người đứng giữa là:

A. Sử dụng các hệ thống IPS/IDS

B. Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên (52 gt)

C. Sử dụng mã hóa để đảm bảo tính bí mật các thông điệp truyền

D. Sử dụng tường lửa để ngăn chặn

48. Các máy tính ma/máy tính bị chiếm quyền điều khiển thường được tin tặc sử dụng để...

A. Gửi các yêu cầu tấn công chèn mã

B. Đánh cắp dữ liệu từ máy chủ cơ sở dữ liệu

C. Gửi thư rác, thư quảng cáo (52 gt)

D. Thực hiện tấn công tràn bộ đệm.

48. Tìm phát biểu sai khi nói về tấn công bằng bomb thư:

A. Là một dạng tấn công DoS khi kẻ tấn công chuyển 1 lượng lớn email đến nạn nhân

B. Có thể thực hiện bằng các kỹ thuật Social Engineering

C. Sử dụng phương pháp truyền tin TCP (79 slide)

D. Có thể được thực hiện bằng cách khai thác lỗi trong hệ thống gửi nhận email SMTP

58. Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau đây trong hệ thống?

A. Máy trạm

B. Người dùng (81 slide)

C. Máy chủ

D. Hệ điều hành & ứng dụng

69. Tấn công kiểu Social Engineering có thể cho phép tin tặc:

A. Đánh cắp toàn bộ dữ liệu trên máy chủ

B. Phá hỏng máy chủ

C. Đánh cắp thông tin nhạy cảm trong cơ sở dữ liệu máy chủ

D. Đánh cắp thông tin nhạy cảm của người dùng (81 slide)

60. Phishing là một dạng của loại tấn công sử dụng...

A. Kỹ thuật chèn mã

B. Kỹ thuật giả mạo địa chỉ IP

C. Kỹ thuật gây tràn bộ đệm

D. Kỹ thuật xã hội (83 slide)

60. Phishing là dạng tấn công vào:

A. Hệ điều hành và các ứng dụng

B. Các hệ thống mạng

C. Các phần mềm máy chủ

D. Người quản trị và người dùng thông thường (83 slide)

44. Pharming là kiểu tấn công vào…

A. Máy chủ web

B. Máy chủ cơ sở dữ liệu của trang web

C. Máy chủ và máy khách web

D. Máy khách/trình duyệt web (86 slide)

61. Các dạng phần mềm độc hại (malware) có khả năng tự nhân bản gồm:

A. Virus, zombie, spyware

B. Virus, trojan, zombie

C. Virus, worm, trojan

D. Virus, worm, zombie (94 slide)

61. Loại mã nguồn độc hại nào có thể được cài đặt song không gây tác hại cho đến khi một hoạt động nào đó được kích hoạt:

A. Sâu

B. Trojan horse (?)

C. Stealth virus

D. Logic bomb (95 slide)

61. Chọn phát biểu đúng về logic bomb:

A. Thường được "nhúng" vào các chương trình đặc trưng và thường tự động "phát nổ" trong một số điều kiện cụ thể

B. Thường "có sẵn" trong các chương trình bình thường và thường tự động "phát nổ" trong một số điều kiện cụ thể

C. Thường được "nhúng" vào các chương trình bình thường

D. Thường được "nhúng" vào các chương trình bình thường và thường hẹn giờ để "phát nổ" trong một số điều kiện cụ thể (95 slide)

65. Trojan horse là chương trình chứa …….., thường giả danh những chương trình ……. nhằm lừa người dùng kích hoạt chúng

A. Mã máy / Có ích

B. Mã máy / Thông dụng

C. Mã độc / Thông dụng

D. Mã độc / Có ích (97 slide)

65. Trojan horses là dạng phần mềm độc hại thường giành quyền truy nhập vào các file của người dùng khai thác cơ chế điều khiển truy nhập...

A. MAC

B. Role-Based

C. Rule-Based

D. DAC (97 slide => Điều khiển truy cập tuỳ quyền (DAC) (Chương 4 – 13 slide))

65. Để thực hiện tấn công bằng Trojan, kẻ tấn công chỉ cần:

A. Cho máy nạn nhân lây nhiễm 1 loại virus bất kì nào đó

B. Thực hiện đồng thời 2 file, 1 file vận hành trên máy nạn nhân, file còn lại hoạt động điều khiển trên máy kẻ tấn công

C. Tạo 1 file chạy vận hành trên máy nạn nhân là đủ (97 slide)

D. Không ý nào đúng

68. Zombie là một chương trình được thiết kế để giành quyền ..... một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để ..... các hệ thống khác.

A. Xâm nhập / Nghe lén

B. Xâm nhập / Tấn công

C. Kiểm soát / Nghe lén

D. Kiểm soát / Tấn công (100 slide)

68. Các zombie thường được tin tặc sử dụng để:

A. Đánh cắp dữ liệu từ máy chủ CSDL

B. Thực hiện tấn công DoS

C. Thực hiện tấn công tràn bộ đệm

D. Thực hiện tấn công DdoS (100 slide)

62. Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình khác là:

A. Ẩn mã của virus

B. Thay thế các chương trình

C. Xáo trộn mã của virus

D. Sửa đổi các chương trình (102 slide)

57. Tìm phát biểu sai trong các phát biểu sau về vòng đời của virus:

A. Giai đoạn "nằm im": Virus trong giai đoạn không được kích hoạt và có thể được kích hoạt nhờ một sự kiện nào đó

B. Giai đoạn phát tán: Virus kiểm soát những chương trình mà nó đã tiếp xúc (104 slide)

C. Giai đoạn kích hoạt: Virus được kích hoạt để thực thi các tác vụ đã được thiết lập sẵn, thường được kích hoạt dựa trên một sự kiện nào đó

D. Giai đoạn thực hiện: thực thi các tác vụ. Một số viruses có thể vô hại, nhưng một số khác có thể xoá dữ liệu, chương trình...

57. Macro viruses là loại viruses thường lây nhiễm vào…

A. Các file tài liệu của bộ phần mềm Open Office

B. Các file tài liệu của bộ phần mềm Microsoft Exchange

C. Các file tài liệu của bộ phần mềm Microsoft SQL

D. Các file tài liệu của bộ phần mềm Microsoft Office (106 slide)

66. Một trong các biện pháp hiệu quả để phòng chống Macro virus:

A. Cấm tự động thực hiện macro trong Microsoft Exchange

B. Sử dụng tường lửa

C. Cấm tự động thực hiện macro trong Microsoft Office (61 gt)

D. Sử dụng IPS/IDS

35. Khác biệt cơ bản của vi rút và sâu là:

A. Vi rút có khả năng tự lây lan mà không cần tương tác của người dùng

B. Sâu có khả năng tự lây lan mà không cần tương tác của người dùng (110 slide)

C. Sâu có khả năng phá hoại lớn hơn

D. Vi rút có khả năng phá hoại lớn hơn

Tổng hợp **(94 slide)**:

- Các phần mềm độc hại cần chương trình chủ, vật chủ (host) để ký sinh và lây nhiễm: Logic bomb, Backdoor, Trojan Horse, Viruses, Rootkit, Adware, Spyware
- Không cần chương trình chủ, vật chủ để lây nhiễm: Worm, Zombie/Bot

50. Một trong các phương thức lây lan thường gặp của sâu mạng là:

A. Lây lan thông qua sao chép các file

B. Lây lan thông qua dịch vụ POP

C. Lây lan thông qua khả năng thực thi từ xa (111 slide)

D. Lây lan thông qua Microsoft Office

50. Đâu không phải một phương pháp lây lan của Worms:

A. Lây lan qua thư điện tử: sử dụng email để gửi bản copy của sâu đến các máy khác

B. Lây lan thông qua khả năng log-in (đăng nhập) từ xa

C. Lây lan thông qua khả năng thực thi từ xa

D. Cần sự đồng ý từ người dùng để lây lan từ máy này sang máy khác (111 slide)

Chương 3: Đảm bảo an toàn thông tin dựa trên mã hoá

3. Một hệ mã hóa gồm các khâu nào?

A. Mã hóa và giải mã (4 slide)

B. Mã hóa và tạo khóa

C. Tạo khóa và phân phối khóa

D. Tạo khóa và giải mã

3. Văn bản sau khi được mã hoá gọi là gì ?

A. Văn bản mã (6 slide)

B. Chứng chỉ

C. Mật mã đối xứng

D. Khoá công khai

5. Như thế nào là một bộ mã hóa thông tin (Cipher) ?

A. Là bản rõ và bản mã

B. Là bộ khóa và chìa để giải mã

C. Là một giải thuật để mã hóa và giải mã thông tin (7 slide)

D. Là một chuỗi dùng trong giải thuật mã hóa và giải mã

5. Như thế nào được gọi là Key ?

A. Là bản rõ và bản mã

B. Là bộ khóa và chìa để giải mã

C. Là một giải thuật để mã hóa và giải mã thông tin

D. Là một chuỗi dùng trong giải thuật mã hóa và giải mã (7 slide)

3. Không gian khoá là gì ?

A. Tổng số khoá có thể có của 1 hệ mã hoá (8 slide)

B. Tổng số khoá công khai của 1 hệ mã hoá

C. Tổng số khoá bí mật của 1 hệ mã hoá

D. Nơi lưu trữ khoá của 1 hệ mã hoá

3. Như nào được gọi là phá mã ?

A. Quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà không cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) và khóa mã (Key). (8 slide)

B. Quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà không cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) nhưng cần có khóa mã (Key).

C. Quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) và khóa mã (Key).

D. Quá trình giải mã thông điệp đã bị mã hóa (ciphertext) cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) nhưng không cần có khóa mã (Key).

11. Mã hoá thông tin có thể được sử dụng để đảm bảo an toàn thông tin trên đường truyền với các thuộc tính:

A. Toàn vẹn, bảo mật, xác thực, trao quyền

B. Toàn vẹn, bảo mật, không thể chối bỏ

C. Toàn vẹn, bí mật, xác thực, không thể chối bỏ (12 slide)

D. Toàn vẹn, bí mật, xác thực, trao quyền

3. Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ thống mật mã ?

A. Hiệu quả (12 slide)

B. Bảo mật

C. Toàn vẹn

D. Không chối từ

5. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm:

A. Phương pháp mã hóa và chia khối

B. Giải thuật mã hóa và ký số

C. Phương pháp mã hóa và không gian khóa (13 slide)

D. Giải thuật mã hóa và giải mã

5. Theo nguyên lý Kerckhoff: “tính an toàn của một hệ mã hoá không nên phục thuộc vào việc giữ bí mật ……, mã chỉ nên phục thuộc vào việc giữ bí mật ……”:

A. khoá mã / giải thuật mã hoá

B. bản mã / khoá mã

C. giải thuật mã hoá / khoá mã (13 slide)

D. bản rõ / bản mã

5. Các yếu tố ảnh hưởng đến quá trình mã hoá:

A. Thời gian thực hiện mã hoá và giải mã

B. Thực hiện mã hoá khối, mở rộng số bit xử lý

C. Thuật toán mã hoá, giải mã và tính an toàn của kênh truyền (69 gt ?)

D. Tất cả đều sai

5. Mã hoá nào sau đây là 1 tiêu chuẩn dùng để phát triển cho việc tạo ra thông điệp an toàn:

A. Digital Signature Standard

B. Secure Hash Algorithm

C. Data Encryption Standard (15 slide)

D. Chữ ký dữ liệu tiêu chuẩn

5. Các giao thức mã hóa và các thuật toán nào sau đây được sử dụng như là nền tảng của hạ tầng cơ sở hạ tầng khóa công khai (PKI):

A. MD5

B. SHA

C. Diffie-Hellman (15 slide)

D. Skipjack

11. Ưu điểm của kỹ thuật mã hoá công khai so với mã hoá khoá bí mật:

A. Có độ an toàn cao hơn

B. Chi phí tính toán thấp hơn

C. Trao đổi khoá dễ dàng hơn (70 gt – 15 slide)

D. Quản lý dễ dàng hơn

6. Trong mã hoá dòng (Stream cipher), dữ liệu được xử lý theo:

A. Từng byte

B. Từng bit

C. Từng chuỗi ký tự

D. Từng bit hoặc từng byte/ ký tự (17 slide)

6. Phát biểu nào sau đây là đúng:

A. Hầu hết các thuật toán mã hoá đối xứng đều dựa trên cấu trúc thuật toán Feistel

B. Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khoá

C. Hầu hết các thuật toán mã hoá khối đều đối xứng (71 gt)

D. Tất cả đều đúng (?)

6. Đâu là các tiêu chuẩn đánh giá một hệ mã hóa:

A. Tính năng, độ bảo mật, chế độ hoạt động, hiệu năng, độ dễ cài đặt

B. Tính năng, độ an toàn, chế độ hoạt động, thuật toán, độ dễ cài đặt

C. Tính năng, độ an toàn, chế độ hoạt động, hiệu năng, độ dễ cài đặt (20 slide)

D. Tính năng, độ an toàn, không gian khóa, hiệu năng, độ dễ cài đặt

6. Đâu là 1 ứng dụng của mã hoá ?

A. PGG

B. GPP

C. PPG

D. PGP (21 slide)

6. Đâu là một phương pháp mã hóa

A. OR

B. AND

C. NOT

D. XOR (22 slide)

6. Đâu là một phương pháp mã hóa

A. Thay thế

B. Đổi chỗ/ hoán vị

C. Vernam

D. Tất cả các đáp án trên (22 slide)

6. Phương pháp Vernam được triển khai như thế nào?

A. Thực hiện sắp xếp lại các giá trị trong một khối để tạo bản mã

B. Thường được dùng trong các bộ phim trinh thám, trong đó việc mã hóa và giải mã sử dụng các khóa mã chứa trong các cuốn sách

C. Sử dụng phép toán logic XOR để tạo bản mã

D. Sử dụng 1 tập ký tự để nối vào các ký tự của bản rõ để tạo bản mã (29 slide)

17. Các giải thuật mã hoá khoá đối xứng:

A. DES, 3-DES, AES (33 slide)

B. DES, RSA, RC4

C. DES, AES, PGP

D. DES, 3-DES, RSA

17. Tìm phát biểu đúng về mã hóa khóa đối xứng (Symmetric key cryptography):

A. Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã (34 slide)

B. Sử dụng một khóa cho quá trình mã hóa và một khóa khác cho giải mã

C. An toàn hơn mã hóa khóa công khai

D. Chỉ sử dụng kỹ thuật mã hóa khối

17. Ở hệ mật mã nào người gửi và nhận thông điệp sử dụng cùng 1 khoá khi mã hoá công khai và giải mã:

A. Đối xứng (34 slide)

B. Không đối xứng

C. RS

D. Difie-Hellman

17. Phát biểu nào đúng với kỹ thuật mã hoá khoá bí mật:

A. Sử dụng 1 mã (key) cho cả quá trính mã hoá và giải mã (34 slide)

B. An toàn hơn mã hoá khoá công khai

C. Chỉ hoạt động theo chế độ mã hoá khối

D. Có thuật toán đơn giản hơn mã hoá công khai

25. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là:

A. Chi phí tính toán lớn

B. Khó khăn trong quản lý và phân phối khóa (34 slide)

C. Độ an toàn thấp

D. Khó khăn trong cài đặt và triển khai hệ thống

17. Yêu cầu đảm bảo sử dụng mã hoá khoá đối xứng:

A. Có thuật toán mã hoá tốt, có 1 khoá bí mật được biết bởi người nhận/ gửi và kênh truyền bí mật để phát khoá (75 gt)

B. Có 1 kênh truyền phù hợp và 1 khoá bí mật được biết bởi người nhận/ gửi

C. Có thuật toán mã hoá tốt và 1 khoá bí mật được biết bởi người nhận/ gửi

D. Tất cả đều đúng

31. Kích thước khoá hiệu dụng của hệ mã hoá DES là:

A. 64 bit

B. 56 bit (36 slide)

C. 128 bit

D. 48 bit

31. Hệ mật DES sử dụng khối khoá được đào tạo bởi:

A. 56 bit ngẫu nhiên

B. 56 bit ngẫu nhiên và 8 bit kiểm tra (36 slide)

C. 64 bit ngẫu nhiên và 8 bit kiểm tra

D. 128 bit ngẫu nhiên

19. Hệ mật DES xử lý từng khối "plain text" có độ dài:

A. 32 bit

B. 64 bit (39 slide)

C. 48 bit

D. 56 bit

19. Sử dụng bao nhiêu bit với DES để có hiệu quả:

A. 56

B. 64 (39 slide ?)

C. 32

D. 16

19. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là:

A. 14

B. 16 (38 slide)

C. 18

D. 20

20. Số lượng các khoá phụ (subkey) cần được tạo ra từ khoá chính trong giải thuật DES là:

A. 12

B. 14

C. 18

D. 16 (41 slide)

20. Trong DES mỗi hàm chọn Si được dùng để:

A. Biến đổi khối dữ liệu mã 48 bit thành 32 bit

B. Biến đổi khối dữ liệu mã 16 bit thành 4 bit

C. Biến đổi khối dữ liệu mã 32 bit thành 4 bit

D. Biến đổi khối dữ liệu mã 6 bit thành 4 bit (41 slide)

20. Các hộp thay thế s-box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là:

A. Vào 4 bít và ra 4 bít

B. Vào 6 bít và ra 6 bít

C. Vào 8 bít và ra 6 bít

D. Vào 6 bít và ra 4 bít (41 slide)

7. Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là 1 chuẩn mã hoá dữ liệu:

A. DSA

B. ECC

C. 3-DES

D. AES (47 slide)

7. Kích thước khối dữ liệu xử lý của giải thuật mã hóa AES là:

A. 160 bit

B. 64 bit

C. 192 bít

D. 128 bit (47 slide)

7. Kích thước khoá có thể có của hệ mã hoá AES là:

A. 64, 128 và 192 bit

B. 128, 256 và 512 bit

C. 128, 256 và 384 bit

D. 128, 160 và 192 bit (47 slide)

24. Giải thuật mã hóa AES được thiết kế dựa trên…

A. mạng hoán vị - vernam

B. mạng xor - thay thế

C. mạng hoán vị - thay thế (47 slide)

D. mạng hoán vị - xor

24. Giải thuật mã hóa AES vận hành dựa trên 1 ma trận 4x4 được gọi là:

A. States

B. Status

C. State (48 slide)

D. Stock

26. Số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã của giải thuật mã hóa AES với khóa 128 bit là:

A. 10 (48 slide)

B. 12

C. 16

D. 14

26. Số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã của giải thuật mã hóa AES với khóa 192 bit là:

A. 10

B. 12 (48 slide)

C. 16

D. 14

26. Trật tự của khâu xử lý trong các vòng lặp chính của giải thuật mã hoá AES là:

A. AddRoundKey, MixColumns, ShiftRows, SubBytes.

B. SubBytes, ShiftRows, MixColumns, AddRoundKey (50 slide)

C. SubBytes, MixColumns, ShiftRows, AddRoundKey

D. AddRoundKey, MixColumns, SubBytes, ShiftRows

26. Bước MixColumns (trộn cột) trong vòng lặp chuyển đổi của hệ mã AES thực hiện việc:

A. Trộn 2 cột kề nhau của ma trận state

B. Mỗi cột của ma trận state được nhân với 1 đa thức (56 slide)

C. Trộn các cột tương ứng của ma trận state với khoá

D. Trộn các dòng tương ứng của ma trận state với khoá

16. Tìm phát biểu đúng về mã hóa khóa bất đối xứng (Asymmetric key cryptography):

A. An toàn hơn mã hóa khóa bí mật

B. Sử dụng 1 khóa cho quá trình mã hóa và 1 khóa khác cho giải mã (59 slide)

C. Chỉ sử dụng kỹ thuật mã hóa khối

D. Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã

16. Nếu muốn xem 1 tài liệu "bảo mật" được mã hoá trên hệ mật bất đối xứng do người khác gửi đến, bạn phải sử dụng khoá nào để giải mã dữ liệu:

A. Khoá công khai của bạn

B. Khoá cá nhân của bạn (59 slide)

C. Khoá cá nhân của bên gửi

D. Khoá công khai của bên gửi

11. Một trong các điểm yếu của các hệ mã hóa khóa công khai là:

A. Khó cài đặt trên thực tế

B. Khó khăn trong quản lý và phân phối khóa

C. Tốc độ chậm (60 slide)

D. Độ an toàn thấp

14. Các hệ mã hoá khoá công khai sử dụng 1 cặp khoá: public key và private key. Yêu cầu đối với 2 khoá này là:

A. Cả 2 khoá đều cần giữ bí mật

B. Có thể công khai private key và cần giữ bí mật public key

C. Có thể công khai public key nhưng phải đảm bảo tính xác thực và cần giữ bí mật private key (83 gt)

D. Có thể công khai public key và cần giữ bí mật private key

14. Độ an toàn của hệ mật mã RSA dựa trên...

A. Độ phức tạp cao của giải thuật RSA

B. Chi phí tính toán lớn

C. Tính khó của việc phân tích số nguyên rất lớn (63 slide)

D. Khóa có kích thước lớn

14. Trong hệ mật mã RSA, quan hệ toán học giữa khoá công khai e và số phi(n) là:

A. Phi(n) là modulo của e

B. e và phi(n) không có quan hệ với nhau

C. e và phi(n) là 2 số nguyên tố cùng nhau (65 slide)

D. Phi(n) là modulo nghịch đảo của e

14. Trong hệ mật mã RSA, quan hệ toán học giữa khoá riêng d và khoá công khai e là:

A. d và e là 2 số nguyên tố cùng nhau

B. d và e không có quan hệ với nhau

C. d là modulo nghịch đảo của e (65 slide)

D. d là modulo của e

14. Trong các cặp khoá sau đây của hệ mật mã RSA với p = 5 và q = 7, cặp khoá nào có khả năng đúng nhất:

A. e = 12, d = 11

B. e = 4, d = 11

C. e = 7, d = 23 (65 slide ?)

D. e = 3, d = 18

Từ đề => phi(n) = 4 * 6 = 24.

Tất cả đáp án đều thoả tính 1 < e < phi(n) nhưng chỉ có C thoả gcd(e, phi(n)) = 1

Nếu vẫn còn đáp án thoả 2 tính chất trên thì xét tiếp d phải thoả (d * e) mod phi(n) = 1

Nhưng đáp án C câu này lại không thoả (d * e) mod phi(n) = 1 ? Đúng hơn thì d = 31 ?

14. Trong giải thuật sinh khoá RSA, với (n, e) là khoá công khai và (n, d) là khoá riêng. Thông điệp bản rõ m đã được chuyển thành số với m < n. Công thức tìm bản mã là:

A. c = m^e mod n (66 slide)

B. c = m^n mod e

C. c = m^d mod n

D. c = n^e mod m

14. Trong giải thuật sinh khoá RSA, với (n, e) là khoá công khai và (n, d) là khoá riêng và bản mã c. Công thức tìm thông điệp bản rõ ứng với c là:

A. m = c^e mod n

B. m = c^n mod d

C. m = c^d mod n (66 slide)

D. m = c^d mod e

15. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước…

A. p càng lớn càng tốt

B. Bằng khoảng một nửa kích thước của modulo n (71 slide)

C. Không có yêu cầu về kích thước của p và q

D. q càng lớn càng tốt

13. Hai thuộc tính cơ bản quan trọng nhất của một hàm băm là:

A. Nén và một chiều

B. Dễ tính toán và có đầu ra cố định

C. Một chiều và đầu ra cố định

D. Nén và dễ tính toán (79 slide)

8. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là:

A. MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa (80 slide)

B. MDC có khả năng chống đụng độ cao hơn MAC

C. MDC an toàn hơn MAC

D. MAC an toàn hơn MDC

8. Khi giá trị hàm băm của 2 thông điệp khác nhau có giá trị tương tự nhau, ta gọi hiện tượng này là:

A. Xung đột (81 slide ?)

B. Tấn công vào ngày sinh

C. Chữ ký số

D. Khoá công khai

8. MAC là từ cấu tạo bằng những chữ đầu của 1 nhóm nào liên quan đến mật mã:

A. Mã xác thực thông điệp (message authentication code) (82 slide)

B. Kiểm soát truy cập bắt buộc (mandatory access control)

C. Kiểm soát truy cập phương tiện (media access control)

D. Các uỷ ban đa tư vấn

21. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi...

A. CheckError

B. CheckTotal

C. CheckNum

D. CheckSum (86 slide)

28. Một trong các ứng dụng phổ biến của các hàm băm một chiều là để...

A. Mã hóa thẻ tín dụng

B. Mã hóa địa chỉ

C. Mã hóa mật khẩu (86 slide)

D. Mã hóa tên tài khoản

21. Thuật giải MD5 cho ta một giá trị băm có độ dài:

A. 64 bit

B. 128 bit (86 slide)

C. 32 bit

D. 256 bit

21. Thuật giải MD5 dùng để:

A. Bảo mật 1 thông điệp

B. Xác thực 1 thông điệp

C. Phân phối khoá mật mã

D. Kiểm tra tính toàn vẹn dữ liệu (86 slide)

2. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là:

A. 14

B. 16 (87 slide)

C. 18

D. 12

2. Thuật giải SHA-1 dùng để:

A. Tạo khoá đối xứng

B. Tạo chữ ký số

C. Tạo 1 giá trị băm độ dài cố định là 256 bit

D. Tạo 1 giá trị băm độ dài cố định là 160 bit (89 slide)

2. Thuật giải SHA:

A. Là hàm băm 1 chiều

B. Dùng cho thuật giải tạo chữ ký số

C. Cho giá trị băm 160 bit

D. Tất cả đều đúng (90 slide ?)

2. Phần xử lý chính của SHA1 làm việc trên 1 chuỗi được gọi là state. Kích thước state là:

A. 150 bit

B. 160 bit (90 slide)

C. 170 bit

D. 180 bit

23. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là:

A. 80 (90 slide)

B. 90

C. 60

D. 70

23. Mỗi vòng xử lý của hàm băm SHA1 bao gồm các thao tác:

A. add - and - or - xor - rotate - mod (90 slide)

B. add - nor - or - xor - rotate - mod

C. sub - and - or - xor - rotate – mod

D. add - and - or - xor - sub – mod

12. Phát biểu nào sau đây về chữ ký số là chính xác:

A. Chữ ký số là một chuỗi dữ liệu được tạo ra bằng cách mã hóa thông điệp sử dụng khóa bí mật

B. Chữ ký số là một chuỗi dữ liệu liên kết với một thông điệp và thực thể tạo ra thông điệp (93 slide)

C. Chữ ký số được sử dụng để đảm bảo tính bí mật và toàn vẹn thông điệp

D. Chữ ký số được sử dụng để đảm bảo tính bí mật, toàn vẹn và xác thực thông điệp

12. Các bước mã hóa của chữ ký điện tử:

A. Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu và nén dữ liệu gởi đi.

B. Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, Sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu. (98 slide)

C. Chỉ sử dụng giải thuật băm để thay đổi thông điệp cần truyền đi và sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên.

D. Tất cả đều đúng

9. Chữ ký số (sử dụng riêng) thường được sử dụng để đảm bảo thuộc tính nào sau đây của thông điệp truyền đưa:

A. Tính bí mật

B. Tính không chối bỏ

C. Tính sẵn dùng

D. Tính toàn vẹn (99 slide)

10. Trong hệ chữ ký số RSA, việc tạo chữ ký số cho một thông điệp cần sử dụng một khóa. Khóa đó là:

A. Khóa riêng của người nhận

B. Khóa công khai của người nhận

C. Khóa công khai của người gửi

D. Khóa riêng của người gửi (100 slide)

10. Trong hệ mã hoá công khai RSA, để tạo 1 chữ ký điện tử của văn bản M ta dùng:

A. S = E(ek, M)

B. S = D(dk, M)

C. S = D(ek, M)

D. S = E(dk, M) (100 slide)

10. Trong hệ mã công khai RSA, ta đã tạo 1 chữ ký điện tử S của văn bản M, khi đó:

A. M = E(ek, S)

B. M = D(dk, S)

C. M = E(dk, S)

D. M = D(ek, S) (100 slide)

10. Sự khác biệt giữa chữ ký số RSA và DSA:

A. RSA an toàn hơn DSA

B. DSA an toàn hơn RSA

C. DSA có chi phí tính toán thấp hơn RSA

D. Giải thuật DSA đơn giản hơn RSA (94 gt ?)

4. Các thuộc tính cơ bản của chứng chỉ số khóa công khai (Public key digital certificate) gồm:

A. Số nhận dạng, khóa riêng của chủ thể, chữ ký của nhà cung cấp

B. Khóa công khai của chủ thể, thông tin địa chỉ chủ thể, thuật toán chữ ký sử dụng

C. Số nhận dạng, khóa riêng của chủ thể, thông tin định danh chủ thể

D. Khóa công khai của chủ thể, thông tin định danh chủ thể, chữ ký của nhà cung cấp (110 slide)

4. Đâu là tên viết tắt của các thành phần của PKI:

A. CA, AB, CD

B. CA, RA, AB

C. CA, AB, VA

D. CA, RA, VA (114 slide)

4. Tổ chức chính cấp phát chứng chỉ được gọi là:

A. CA (114 slide)

B. RA

C. LRA

D. VA

4. Tính hợp lệ của 1 chứng chỉ dựa vào điều gì ?

A. Tính hợp lệ của Quyền cấp chứng chỉ (114 slide)

B. Tính hợp lệ của người sở hữu

C. Tính hợp lệ của khoá công khai

D. Giai đoạn chứng chỉ được sử dụng

4. Hầu hết định dạng chứng chỉ công cộng được sử dụng trong môi trường PKI là gì ?

A. X.509 (98 gt)

B. X.508

C. RSA

D. PKE

3. Giao thức SSL dùng để:

A. Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP

B. Cung cấp bảo mật cho thư điện tử

C. Cung cấp bảo mật cho web (150 slide)

D. Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Platform Window

3. Giao thức bảo mật SSL đảm bảo tính bí mật, toàn vẹn và xác thực thông điệp bằng các kỹ thuật nào sau đây:

A. Mã hóa khóa bí mật và chữ ký số

B. Mã hóa khóa bí mật và mã hóa khóa công khai

C. Mã hóa khóa bí mật và hàm băm có khóa MAC (151 slide)

D. Mã hóa khóa bí mật và hàm băm không khóa MDC

3. Giao thức SSL sử dụng giao thức con SSL Handshake để khởi tạo phiên làm việc. SSL Handshake thực hiện việc trao đổi các khóa phiên dùng cho phiên làm việc dựa trên:

A. Chữ ký số

B. Mã hóa khóa bí mật

C. Mã hóa khóa công khai (151 slide)

D. Chứng chỉ số

29. Giao thức SSL sử dụng giao thức con SSL Handshake để khởi tạo phiên làm việc. SSL Handshake thực hiện việc xác thực thực thể dựa trên:

A. Chứng chỉ số khóa công khai (151 slide)

B. Mã hóa khóa bí mật

C. Mã hóa khóa công khai

D. Chữ ký số

1. PGP đảm bảo tính bí mật thông điệp bằng cách sử dụng:

A. Mã hóa khóa bất đối xứng sử dụng khóa phiên

B. Mã hóa khóa đối xứng sử dụng khóa phiên

C. Mã hóa khóa bất đối xứng sử dụng khóa công khai (160 slide)

D. Mã hóa khóa đối xứng sử dụng khóa công khai

30. PGP đảm bảo tính xác thực thông điệp bằng cách:

A. Mã hóa/giải mã thông điệp

B. Sử dụng hàm băm có khóa MAC

C. Sử dụng hàm băm không khóa MDC

D. Tạo và kiểm tra chữ ký số (160 slide)

30. PGP là giao thức để xác thực:

A. Quyền đăng cập vào hệ thống máy chủ Window

B. Thực hiện mã hóa thông điệp theo thuật tóan RSA

C. Địa chỉ của máy trạm khi kết nối vào Internet

D. Bảo mật cho thư điện tử (110 gt)

18. Sử dụng kết hợp chứng chỉ số khóa công khai và chữ ký số có thể đảm bảo:

A. Xác thực thực thể và toàn vẹn thông tin truyền (165 slide)

B. Xác thực thực thể và bí mật thông tin truyền

C. Bí mật và xác thực nguồn gốc thông tin truyền

D. Bí mật và toàn vẹn thông tin truyền

Chương 4: Các kỹ thuật và công nghệ đảm bảo an toàn thông tin

30. Một hệ thống điều khiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây ?

A. Xác thực, trao quyền và quản trị (10 slide)

B. Xác thực, đăng nhập và trao quyền

C. Xác thực, đăng nhập và kiểm toán

D. Xác thực, trao quyền và kiểm toán

30. Hai dịch vụ quan trọng nhất của một hệ thống điều khiển truy nhập là:

A. Authentication và Authorization (10 slide)

B. Authenticator và Administrator

C. Administrator và Authorization

D. Authentication và Administrator

32. Tìm phát biểu đúng về dịch vụ xác thực trong điều khiển truy nhập:

A. Là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người dùng cung cấp (10 slide)

B. Là quá trình xác minh nhận dạng của chủ thể

C. Là quá trình xác minh các thông tin nhận dạng của chủ thể yêu cầu truy nhập đối tượng

D. Là quá trình xác minh nhận dạng của người dùng

30. Một điểm yếu điển hình trong hệ thống điều khiển truy nhập là việc sử dụng mật khẩu dễ đoán hoặc mật khẩu được lưu ở dạng rõ. Đây là điểm yếu thuộc khâu:

A. Xác thực (10 slide)

B. Trao quyền

C. Xác thực và trao quyền

D. Quản trị

30. Phương pháp quét võng mạc thích hợp nhất đối với dịch vụ nào sau đây ?

A. Xác thực (10 slide)

B. Kiểm định

C. Kiểm soát truy cập

D. Bảo mật dữ liệu

27. Mục đích chính của điều khiển truy nhập là để đảm bảo các thuộc tính an ninh của thông tin, hệ thống và các tài nguyên, gồm:

A. Tính bảo mật, tính toàn vẹn và tính xác thực

B. Tính bí mật, tính toàn vẹn và tính xác thực

C. Tính bảo mật, tính toàn vẹn và tính sẵn dùng

D. Tính bí mật, tính toàn vẹn và tính sẵn dùng (11 slide)

26. Ba cơ chế điều khiển truy nhập thông dụng gồm:

A. DAC, MAC và RRAC

B. DAC, BAC và RBAC

C. DAC, MAC và BAC

D. DAC, MAC và RBAC (12 slide)

10. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập DAC:

A. DAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác (14 slide)

B. DAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

C. DAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất

D. DAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác

33. Loại tấn công nào sau đây chiếm quyền truy nhập đến tài nguyên lợi dụng cơ chế điều khiển truy nhập DAC?

A. Spoofing

B. Trojan horse (15 slide c4 + 97 slide c2)

C. Man in the middle

D. Phishing

12. ACL là tên viết tắt của:

A. Arbitrary Code Language

B. Access Control Library

C. Allowed Control List

D. Access Control List (18 slide)

12. Danh sách điều khiển truy nhập ACL thực hiện việc quản lý quyền truy nhập đến các đối tượng cho người dùng bằng cách:

A. Các quyền truy nhập vào đối tượng cho mỗi người dùng được quản lý trong một ma trận

B. Các quyền truy nhập vào đối tượng cho mỗi người dùng được quản lý riêng rẽ

C. Mỗi người dùng được gán một danh sách các đối tượng kèm theo quyền truy nhập

D. Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập (18 slide)

17. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập bắt buộc MAC:

A. MAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác

B. MAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác

C. MAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị (20 slide)

D. MAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất

17. Các mức độ nhạy cảm của thông tin được chia từ cao xuống thấp đối với an ninh quốc gia là:

A. Tuyệt mật (Secret – S), Tối mật (Top Secret – T), Mật (Confidential – C), Không phân loại (Unclassified – U)

A. Không phân loại (Unclassified – U), Tuyệt mật (Secret – S), Tối mật (Top Secret – T), Mật (Confidential – C)

A. Không phân loại (Unclassified – U), Tối mật (Top Secret – T), Tuyệt mật (Secret – S), Mật (Confidential – C)

A. Tối mật (Top Secret – T), Tuyệt mật (Secret – S), Mật (Confidential – C), Không phân loại (Unclassified – U) (21 slide)

1. Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula là:

A. Đọc lên và ghi lên

B. Đọc xuống và ghi xuống

C. Đọc xuống và ghi lên (25, 26 slide)

D. Đọc lên và ghi xuống

9. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập dựa trên vai trò - RBAC:

A. RBAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác

B. RBAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất

C. RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức (28 slide)

D. RBAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

9. Điều khiển truy nhập dựa trên luật (Rule-Based access control) được sử dụng phổ biến trong:

A. VPN

B. SSL/TLS

C. Firewall (33 slide)

D. Kerberos

2. Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên:

A. Tần suất sử dụng mật khẩu

B. Kích thước của mật khẩu

C. Độ khó đoán và tuổi thọ của mật khẩu (36 slide)

D. Số loại ký tự dùng trong mật khẩu

36. Ưu điểm của mật khẩu một lần (OTP-One Time Password) so với mật khẩu truyền thống là:

A. Chống được tấn công từ điển

B. Chống được tấn công vét cạn

C. Chống được tấn công phá mã

D. Chống được tấn công phát lại (37 slide)

21. Một trong các dạng khóa mã (encrypted keys) được sử dụng rộng rãi trong điều khiển truy nhập là:

A. E-token

B. Chứng chỉ số khóa công khai (38 slide)

C. The ATM

D. Mobile-token

28. Số lượng nhân tố (factor) xác thực sử dụng trong điều khiển truy nhập dựa trên thẻ thông minh là:

A. 1

B. 2 (42 slide)

C. 3

D. 4

34. Yếu tố nào cần được sử dụng kết hợp với 1 thẻ thông minh để xác thực?

A. Quét võng mạc

B. Thẻ nhớ

C. Số PIN (42 slide)

D. Mã hoá khoá

23. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smart card) trong điều khiển truy nhập là:

A. Có cơ chế xác thực mạnh hơn (46 slide)

B. Có cơ chế xác thực đa dạng hơn

C. Được sử dụng rộng rãi hơn

D. Có chi phí rẻ hơn

19. Ví điện tử Paypal là một dạng...

A. Khóa mã (encrypted key)

B. The ATM

C. Thẻ bài (token) (48 slide)

D. Thẻ thông minh (smart card)

24. Phương pháp xác thực nào dưới đây có thể cung cấp khả năng xác thực có độ an toàn cao nhất?

A. Sử dụng Smartcard

B. Sử dụng vân tay (51 slide)

C. Sử dụng chứng chỉ số

D. Sử dụng mật khẩu

6. Ưu điểm của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là:

A. Bảo mật cao và độ ổn định cao

B. Bảo mật cao và chi phí thấp

C. Bảo mật cao và luôn đi cùng với chủ thể (51 slide)

D. Bảo mật cao và được hỗ trợ rộng rãi

35. Một trong các nhược điểm chính của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học:

A. Không được hỗ trợ rộng rãi

B. Chi phí đắt (51 slide)

C. Khó sử dụng

D. Công nghệ phức tạp

18. Thiết bị nào sử dụng bộ lọc gói và các quy tắc truy cập để kiểm soát truy cập đến các mạng riêng từ các mạng công cộng , như là Internet ?

A. Điểm truy cập không dây

B. Router

C. Switch

D. Tường lửa (126 gt)

18. Cho biết câu nào đúng trong các câu ?

A. Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm

B. Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn

C. Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập

D. Tất cả đều đúng (126 gt)

18. Đâu là một loại tường lửa?

A. Server gateway

B. Application server

C. Application-level gateway (63 slide)

D. Gateway server

18. Loại Firewall nào sau đây cho phép hoạt động ở lớp phiên (session) của mô hình OSI?

A. Packet filtering firewall (lớp mạng)

B. Application level firewall (lớp ứng dụng)

C. Circuit level firewall (lớp phiên) (63 slide)

D. Stateful multilayer inspection firewall

15. Tường lửa lọc gói có thể lọc các thông tin nào trong gói tin?

A. Chỉ các thông tin trong header của gói tin (128 gt)

B. Chỉ các thông tin trong payload của gói tin

C. Chỉ lọc địa chỉ IP trong gói tin

D. Cả thông tin trong header và payload của gói tin

7. Một ưu điểm của tường lửa có trạng thái so với tường lửa không trạng thái là:

A. Lọc nội dung gói tốt hơn

B. Nhận dạng được các dạng tấn công và các phần mềm độc hại

C. Chạy nhanh hơn

D. Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau (67, 69 slide)

25. Đâu là các tính năng của kiểm soát truy nhập sử dụng tường lửa?

A. Kiểm soát dịch vụ và các phần mềm

B. Kiểm soát người dùng và tin tặc

C. Kiểm soát dịch vụ và hướng (70 slide)

D. Kiểm soát virus và các malware khác

13. Tường lửa không thể chống lại...

A. Các hiểm họa từ bên trong (71 slide)

B. Các hiểm họa từ bên ngoài

C. Tấn công giả mạo địa chỉ

D. Tấn công từ mạng Internet

34. Đâu là tên viết đúng của Hệ thống phát hiện đột nhập/xâm nhập?

A. Intrusion Detector System

B. Intrusion Detecting System

C. Intrusion Detection System (72 slide)

D. Instruction Detection System

29. Một nhiệm vụ chính của các hệ thống IDS/IPS là:

A. Truy tìm và tấn công ngược lại hệ thống của tin tặc

B. Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập (74 slide)

C. Giám sát lưu lượng mạng nhận dạng các dấu hiệu của tấn công, xâm nhập

D. Giám sát các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập

14. Sau khi cố gắng login đến một trạm làm việc trong 3 lần, một user thấy đã bị khóa bên ngoài hệ thống và không thể thực hiện bất kỳ nỗ lực nào hơn nữa. Vấn đề này phù hợp nhất với điều gì:

A. Cổng mạng disable

B. Hệ thống phát hiện xâm nhập disable tài khoản của user (75 slide)

C. Tường lửa disable khi truy cập đến host

D. User quên mật khẩu của họ

14. Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là:

A. IPS phát hiện xâm nhập hiệu quả hơn

B. IPS có khả năng chủ động ngăn chặn xâm nhập (75 slide)

C. IDS phát hiện xâm nhập hiệu quả hơn

D. IDS có khả năng chủ động ngăn chặn xâm nhập

14. Các hệ thống phát hiện xâm nhập có thể thu thập dữ liệu đầu vào từ:

A. Các host

B. Mạng và các host (78 slide)

C. Mạng

D. Các router

14. Hệ thống nào được cài đặt trên Host để cung cấp 1 tính năng IDS ?

A. Network sniffer

B. H-IDS (Host-based IDS) (78 slide)

C. N-IDS (Network-based IDS)

D. VPN

22. Tại sao một hệ thống phát hiện xâm nhập dựa trên chữ ký không thể phát hiện các tấn công, xâm nhập mới?

A. Do chữ ký của chúng chưa tồn tại trong hệ thống (85 slide)

B. Do các tấn công, xâm nhập mới không có chữ ký

C. Do các tấn công, xâm nhập mới không gây ra bất thường

D. Do các tấn công, xâm nhập mới chỉ gây thiệt hại nhỏ

5. Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết:

A. Các hành vi tấn công xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường (86 slide)

B. Các hành vi tấn công, xâm nhập gây ngắt quãng dịch vụ cung cấp cho người dùng

C. Các hành vi tấn công xâm nhập có quan hệ chặt chẽ với các dịch vụ được cung cấp

D. Các hành vi tấn công, xâm nhập gây tổn hại nghiêm trọng cho hệ thống

3. Phát hiện tấn công, xâm nhập dựa trên bất thường có tiềm năng phát hiện các loại tấn công, xâm nhập mới là do:

A. Không yêu cầu biết trước thông tin về chúng (89 slide)

B. Đã có chữ ký của các tấn công, xâm nhập mới

C. Các tấn công, xâm nhập mới thường dễ nhận biết

D. Không yêu cầu xây dựng cơ sở dữ liệu các chữ ký

4. Một trong các điểm yếu làm giảm hiệu quả của phát hiện tấn công, xâm nhập dựa trên bất thường là:

A. Không có khả năng ngăn chặn tấn công, đột nhập

B. Không có khả năng phát hiện các cuộc tấn công Dos

C. Tỷ lệ cảnh báo sai cao (89 slide)

D. Không có khả năng phát hiện tấn công, xâm nhập mới

31. Tìm phát biểu đúng về phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường:

A. Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn (89 slide)

B. Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng thấp hơn

C. Phát hiện xâm nhập dựa trên bất thường có tỷ lệ phát hiện đúng cao hơn

D. Hai cách phát hiện có tỷ lệ phát hiện tương đương nhau

8. Các phương pháp xử lý, phân tích dữ liệu và mô hình hoá trong phát hiện tấn công, xâm nhập dựa trên bất thường, gồm:

A. Thống kê, học máy, khai phá dữ liệu (90 slide)

B. Học máy, khai phá dữ liệu, agents

C. Thống kê, học máy, đồ thị

D. Thống kê, đối sánh chuỗi, đồ thị

Chương 5: Quản lý, chính sách và pháp luật an toàn thông tin

16. Phát biểu đúng khi nói về tài sản an toàn thông tin ?

A. Tài sản an toàn thông tin là thông tin, thiết bị, hoặc các thành phần khác hỗ trợ các hoạt động có liên quan đến thông tin.

B. Tài sản an toàn thông tin có thể gồm phần cứng, phần mềm và thông tin

C. A và B đều đúng (4 slide)

D. A và B đều sai

16. Quản lý an toàn thông tin (Information security management) là một tiến trình (process) nhằm …….. các tài sản quan trọng của cơ quan, tổ chức, doanh nghiệp được bảo vệ ……..... với ……...:

A. Đảm bảo / Đầy đủ / Chi phí phù hợp (5 slide)

B. Chắc chắn / Toàn diện / Chi phí phù hợp

C. Chắc chắn / Đầy đủ / Chi phí rẻ

D. Đảm bảo / Toàn diện / Chi phí rẻ

16. Đâu là phương pháp tiếp cận đánh giá rủi ro ?

A. Tất cả các đáp án trên (10 slide)

B. Phương pháp đường cơ sở

C. Phương pháp phân tích chi tiết rủi ro

D. Phương pháp không chính thức

16. Các bước thực hiện 3 phương pháp đánh giá rủi ro an toàn thông tin của phương pháp kết hợp:

A. Đường cơ sở - chính thức – chi tiết

B. Không chính thức - đường cơ sở – chi tiết

C. Đường cơ sở - không chính thức – chi tiết (17 slide)

D. Không chính thức – chi tiết – đường cơ sở

16. Các phương pháp đánh giá rủi ro an toàn thông tin phù hợp với các tổ chức có hệ thống công nghệ thông tin theo thứ tự: quy mô nhỏ - quy mô nhỏ và vừa – quy mô vừa và lớn - quy mô lớn:

A. Đường cơ sở - Không chính thức – Phân tích chi tiết rủi ro – Kết hợp

B. Không chính thức - Đường cơ sở – Phân tích chi tiết rủi ro – Kết hợp

C. Đường cơ sở - Không chính thức – Kết hợp - Phân tích chi tiết rủi ro (12, 14, 16, 19 slide)

D. Không chính thức - Đường cơ sở – Kết hợp - Phân tích chi tiết rủi ro

16. Luật gồm những điều khoản bắt buộc hoặc cấm những hành vi cụ thể. Các điều luật thường được xây dựng từ các vấn đề:

A. Xã hội

B. Văn hoá

C. Đạo đức (32 slide)

D. Quốc tế

16. Chính sách bảo mật là:

A. Cơ chế mặc định của hệ điều hành

B. Các tập luật được xây dựng nhằm bảo vệ khỏi các tấn công bất hợp pháp bên ngoài

C. Phương thức xác định các hành vi "phù hợp" của các đối tượng tương tác với hệ thống (34 slide)

D. Tất cả đều đúng

Chương ?: Ngoài giáo trình và slide

16. Các thành phần chính của hệ thống máy tính gồm:

A. CPU, Bộ nhớ, HDD, hệ điều hành và các ứng dụng

B. CPU, hệ điều hành và các ứng dụng

C. Hệ thống phần cứng và Hệ thống phần mềm

D. CPU, Bộ nhớ, HDD và Hệ thống bus truyền dẫn

3. Nội dung nào sau đây không cần sử dụng mật mã ?

A. Toàn vẹn (?)

B. Truy cập (!)

C. Bảo mật

D. Xác thực

3. Quản trị văn phòng của bạn đang được huấn luyện để thực hiện sao lưu máy chủ. Phương pháp xác thực nào là lý tưởng đối với tình huống này ?

A. MAC (?)

B. DAC

C. Các mã thông báo bảo mật

D. RBAC

3. Các loại khoá mật mã nào dễ bị crack nhất ?

A. 40 bit (?)

B. 56 bit

C. 128 bit

D. 256 bit

16. Không nên sử dụng nhiều hơn 1 phần mềm quét virus chạy ở chế độ quét theo thời gian thực trên một máy tính vì:

A. Các phần mềm quét virus xung đột với nhau

B. Các phần mềm quét virus không thể hoạt động

C. Các phần mềm quét virus chiếm nhiều tài nguyên

D. Các phần mềm quét virus tấn công lẫn nhau

20. Dạng xác thực sử dụng các thông tin nào dưới đây đảm bảo độ an toàn cao hơn?

A. Thẻ ATM và tên truy nhập

B. Tên truy nhập và số PIN

C. Thẻ ATM và số PIN

D. Tên truy nhập và mật khẩu

20. Để đảm bảo an toàn cho hệ thống điều khiển truy cập, 1 trong các biện pháp phòng chống hiệu quả là ?

A. Không mở các email của người lạ hoặc email quảng cáo

B. Không cho phép chạy các chương trình điều khiển từ xa

C. Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng

D. Không cài đặt và chạy các chương trình tải từ các nguồn không tin cậy

20. Sau khi 1 user đã được định danh (identified), điều gì cần phải làm trước khi họ log vào 1 mạng máy tính ?

A. Phải nhập user ID đã được mã hoá

B. Được phép truy cập với mức ưu tiên được thiết lập

C. Xác thực với mật khẩu (?)

D. Người quản trị phải enable để gõ vào

20. Sau khi 1 user đã được định danh và xác thực hệ thống, để cho phép user sử dụng tài nguyên user cần phải được:

A. Được truyền lại

B. Được mã hoá

C. Được uỷ quyền

D. Được enable

20. Các hệ điều hành Windows và Linux sử dụng các mô hình điều khiển truy cập nào dưới đây ?

A. DAC và MAC

B. MAC và Role-BAC

C. DAC và Role-BAC

D. MAC và Rule-BAC

33. Đối với Firewall lọc gói, hình thức tấn công nào sau đây được thực hiện ?

A. Nhái địa chỉ IP, tấn công giữa, tấn công biên

B. Nhái địa chỉ IP, tấn công đường đi nguồn, tấn công từng mẫu nhỏ

C. Nhái địa chỉ IP, tấn công vượt firewall, tấn công từng mẫu nhỏ

D. Nhái địa chỉ IP, tấn công vượt firewall, tấn công đường đi nguồn

33. Nên cài mức truy cập mặc định là mức nào sau đây ?

A. No access

B. Read access

C. Write access

D. Full access

33. Để đánh giá điểm mạnh của hệ thống IDS người ta dựa vào các yếu tố:

A. Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp

B. Khởi sự, cách thực hiện, biểu hiện mà nó ghi nhận

C. Cách thực hiện, biểu hiện mà nó ghi nhận, những đặc trưng ghép nối hoặc tích hợp

D. Tất cả đều đúng

33. Qui trình quyết định giá trị của thông tin hay thiết bị trong một tổ chức được gọi là gì?

A. Đánh giá tài nguyên thông tin

B. Nhận dạng chuỗi

C. Đánh giá rủi ro

D. Quét các điểm yếu

33. Khi được hỏi về các mối đe dọa cho công ty từ phía các hacker. Loại thông tin nào sau đây sẽ giúp ích nhiều nhất ?

A. Các điểm yếu

B. Nhận dạng mối đe dọa

C. Đánh giá rủi ro

D. Xác minh tài sản sở hữu

33. Một đêm làm việc khuya và bạn phát hiện rằng ổ cứng của bạn hoạt động rất tích cực mặc dù bạn không thực hiện bất kỳ thao tác nào trên máy tính. Bạn nghi ngờ điều gì?

A. Một virus đang phát tán rộng trong hệ thống

B. Khả năng ổ đĩa ngừng hoạt động sắp xảy ra

C. Hệ thống của bạn đang chịu tác động của tấn công DoS

D. Tấn công TCP/IP hijacking đang cố gắng thực hiện

33. Khái niệm nào sau đây được dùng để xác định chuẩn thực thi các hệ thống mã hóa diện rộng?

A. PKI

B. Đối xứng

C. Không đối xứng

D. PKE

33. Nguyên nhân chính của lỗ hổng an ninh cho phép tấn công thực hiện mã từ xa là:

A. Lỗi lập trình phần mềm

B. Lỗi thiết kế phần mềm

C. Lỗi tích hợp hệ thống

D. Lỗi quản trị hệ thống

33. Bộ lọc gói thực hiện chức năng nào ?

A. Ngăn chặn các gói trái phép đi vào từ mạng bên ngoài

B. Cho phép tất cả các gói rời mạng

C. Cho phép tất cả các gói đi vào mạng

D. Loại trừ sự xung đột trong mạng

33. Trong các phát biểu sau đây phát biểu nào là đúng nhất ?

A. Firewall là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công

B. Firewall là một điểm chặn của hệ thống trong quá trình điều khiển và giám sát

C. Firewall là một phần mềm hoặc phần cứng có khả năng ngăn chặn tấn công từ bên trong và bên ngoài vào hệ thống.

D. Firewall là một giải pháp giúp hệ thống phát hiện và ngăn chặn các truy cập trái phép

34. Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị tấn công từ bên ngoài ?

A. Đăng nhập hệ thống (System logs)

B. Kerberos

C. Sinh trắc học

D. Phần mềm antivirus