

CK.0000071480

TRẦN CÔNG HÙNG

Q

Quản trị và bảo mật Mạng không dây



ic
PUBLISHER

NHÀ XUẤT BẢN
THÔNG TIN VÀ TRUYỀN THÔNG

YÊN
U

Quản trị và bảo mật

Mạng không dây

PGS.TS. TRẦN CÔNG HÙNG

Quản trị và bảo mật
Mạng không dây

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

1910
MAY 10 1910
RECEIVED
LIBRARY OF THE
MUSEUM OF COMPARATIVE ZOOLOGY
AND ANATOMY
HARVARD UNIVERSITY

LỜI NÓI ĐẦU

Quản trị và bảo mật mạng là một lĩnh vực vô cùng rộng lớn. Do đó, trong khuôn khổ quyển sách, tác giả chỉ đi sâu nghiên cứu kỹ một khía cạnh của quản trị mạng không dây và bảo mật mạng, đó là *các thuật toán mật mã* - vì đây chính là nền tảng cốt lõi nhất.

Trong quyển sách này trình bày các kỹ thuật mật mã được phổ biến rộng rãi như DES, RSA, ECC... Bên cạnh việc nghiên cứu nguyên lý hoạt động, tác giả sẽ phân tích các điểm mạnh và điểm yếu của các thuật toán cùng phương pháp tấn công chúng. Song song đó, tác giả còn bổ sung một số thuật toán khác để hiểu thêm về các cách thức mã hóa dữ liệu.

Ngoài các thuật toán mật mã, quyển sách cũng giới thiệu một số hệ thống truyền thông không dây, đặc biệt là hệ thống thông tin di động toàn cầu (GSM). Tác giả sẽ phân tích sự phù hợp của từng thuật toán cho các hệ thống này rồi từ đó chọn ra một thuật toán tốt nhất, áp dụng cho hệ thống GSM...

Nội dung quyển sách gồm 17 chương, cụ thể như sau:

Chương 1: Giới thiệu mật mã

Chương 2: Một số thuật toán mật mã

Chương 3: Tổng quan về hệ thống GSM

Chương 4: Các thuật toán mật mã hiện dùng trong GSM

Chương 5: Tấn công các thuật toán mật mã

Chương 6: Áp dụng các thuật toán mật mã vào hệ thống GSM

Chương 7: Mạng không dây

Chương 8: Các thiết bị hạ tầng mạng không dây

Chương 9: Bảo mật mạng không dây

Chương 10: Tìm hiểu IDS trong LAN và IDS trong mạng không dây

Chương 11: Cấu hình trong mạng không dây

Chương 12: Thiết kế hệ thống phát hiện xâm nhập WIDSPro

Chương 13: Tìm hiểu về VPN

Chương 14: Giao thức bảo mật SSL

Chương 15: Tìm hiểu về OpenVPN

Chương 16: Triển khai mạng VPN sử dụng hệ thống OpenVPN

Chương 17: Xây dựng công cụ triển khai OpenVPN

Quản trị và bảo mật mạng không dây là môn học quan trọng tại Học viện Công nghệ Bưu chính Viễn thông nói riêng và các trường đại học có chuyên ngành Điện tử Viễn thông và Công nghệ Thông tin nói chung. Ngoài ra, quyển sách còn là tài liệu tham khảo thiết yếu để phục vụ cho các kỹ sư và nghiên cứu sinh trong công tác chuyên môn.

Trong quá trình biên soạn, mặc dù tác giả đã có nhiều cố gắng song khó tránh khỏi những thiếu sót, rất mong nhận được sự cảm thông và ý kiến đóng góp của quý vị độc giả để lần xuất bản sau sẽ bổ sung hoàn chỉnh hơn.

Mọi ý kiến đóng góp xin gửi qua e-mail: conghung@ptithcm.edu.vn.

Xin trân trọng giới thiệu cùng bạn đọc.

TP.HCM, tháng 4 năm 2013

PGS.TS. Trần Công Hùng

MỤC LỤC

<i>Lời nói đầu</i>	5
<i>Mục lục</i>	7
Chương 1: GIỚI THIỆU MẬT MÃ	15
1.1. Giới thiệu tổng quan về mật mã.....	15
1.2. Mã hóa số liệu (Data Encoding).....	16
1.2.1. Mã NRZ (Non Return to Zero).....	17
1.2.2. Mã nhị pha.....	17
1.2.3. Mã Miller.....	18
1.2.4. Mã nhị phân đa mức.....	20
1.2.5. Mã HDBn (High Density Bipolar n).....	20
1.3. Phát hiện và sửa sai.....	21
1.3.1. LRC.....	22
1.3.2. CRC.....	22
1.3.3. Mã sửa sai Hamming.....	25
1.3.4. Mã Nén Huffman.....	26
Chương 2: MỘT SỐ THUẬT TOÁN MẬT MÃ	29
2.1. Khái niệm chung.....	29
2.2. Sự tương quan giữa ổ khóa và chìa khóa.....	31
2.3. Phân loại các thuật toán mật mã.....	32
2.4. Các cách mã hóa cơ bản.....	32
2.4.1. Nguyên lý Kerckhoff.....	32
2.4.2. Mật mã hoán vị.....	33
2.4.3. Mật mã thay thế.....	33
2.4.4. Mật mã hỗn hợp.....	34
2.5. Hệ thống mật mã DES.....	35
2.5.1. Cấu trúc hệ thống DES.....	35
2.5.2. Phân tích và thiết kế S-box.....	42
2.5.3. Khảo sát sự phụ thuộc của dữ liệu.....	46
2.5.4. Các hệ thống DES trong thực tế.....	53

2.6. Hệ thống RSA	58
2.6.1. Cấu trúc hệ thống RSA	58
2.6.2. Phân tích đặc điểm của hệ thống RSA	59
2.7. Hệ thống mật mã Merkle Hellman Knapsack	61
2.8. Hệ thống mật mã dạng Ellip (ECC)	66
2.8.1. Nguyên lý hoạt động của thuật toán	66
2.8.2. Khả năng bảo mật của thuật toán	70
2.9. MD4, MD5	70
2.10. Thuật toán SHA	73
2.10.1. Giới thiệu tổng quan	73
2.10.2. Một số đặc điểm của các thuật toán SHA	74
2.10.3. Các phép toán được dùng trong thuật toán SHA	74
2.10.4. Các hàm và hằng số được sử dụng trong thuật toán SHA	75
2.10.5. Quá trình tiền xử lý	77
2.10.6. Thuật toán băm	80
2.11. Các thuật toán dùng để xác thực	115
2.11.1. Hệ thống Elgamal	116
2.11.2. Dạng thức khác của hệ thống Elgamal	118
2.11.3. Hệ thống Ong-Schnorr-Shamir (OSS)	119
2.11.4. Dạng thức khác của hệ thống OSS	120
2.12. Quản lý khóa	122
2.12.1. Giới thiệu về cấu trúc hệ thống quản lý khóa	122
2.12.2. Quy trình tạo khóa	123
2.12.3. Quy trình phân phối khóa	124
Chương 3: TỔNG QUAN VỀ HỆ THỐNG GSM	129
3.1. Cấu trúc tổng quát của hệ thống GSM	129
3.1.1. Trạm di động (MS)	129
3.1.2. Hệ thống trạm gốc (BS)	130
3.1.3. Hệ thống chuyển mạch mạng (NSS)	131
3.1.4. Hệ thống khai thác bảo dưỡng (OSS)	131
3.2. Mô hình OSI của hệ thống GSM	132
Chương 4: CÁC THUẬT TOÁN MẬT MÃ HIỆN DÙNG TRONG GSM	133
4.1. Các đặc điểm bảo mật của hệ thống GSM	133
4.1.1. Trung tâm xác thực (AuC)	134