

Các vấn đề về bảo mật với hệ thống mạng

không dây : Luận văn ThS / Đinh Tuấn Long ; Nghd. :

PGS.TS. Nguyễn Gia Hiểu . - H. : ĐHCN, 2006 . - 92 tr. +
CD-ROM

Tóm tắt: Giới thiệu tổng quan về công nghệ không dây, công nghệ trải phổ, chuẩn IEEE 802.11 cho mạng không dây, mô hình hoạt động mạng không dây và một số thành phần kỹ thuật khác. Nêu lên các yếu điểm của mạng không dây và các phương thức tấn công mạng. Từ đó đưa ra các giải pháp bảo mật truyền thống, các giải pháp bảo mật cơ bản cũng như chuẩn bảo mật WPA2 cho mạng không dây

MỞ ĐẦU

CHƯƠNG 1 – TỔNG QUAN VỀ MẠNG KHÔNG DÂY	1
1 – Giới thiệu	1
2 – Công nghệ trải phổ	2
2.1 – Công nghệ trải phổ trực tiếp DSSS	4
2.2 – Công nghệ trải phổ nhảy tần số FHSS	5
3 – Chuẩn IEEE 802.11 cho mạng không dây	7
3.1 – IEEE 802.11	7
3.2 – IEEE 802.11b	8
3.3 – IEEE 802.11a	10
3.4 – IEEE 802.11g	11

3.5 – IEEE 802.11e	12
3.6 – Các đặc tả khác	12
4 – Mô hình hoạt động mạng không dây	12
4.1 – Phương thức Ad Hoc	13
4.2 – Phương thức tập dịch vụ cơ bản BSS	14
5 – Một số thành phần kỹ thuật khác	16
5.1 – Đa truy cập cảm ứng sóng mang/ Tránh xung đột CSMA/CA	16
5.2 – Yêu cầu và sẵn sàng gửi RTS/CTS	17
5.3 – Phân mảnh	17
CHƯƠNG 2 - CÁC YẾU ĐIỂM CỦA MẠNG KHÔNG DÂY –	
CÁC PHƯƠNG PHÁP TẤN CÔNG MẠNG	18
1 – Yếu điểm của sự không dây	18
2 – Phương thức bảo mật WEP – Wired Equivalent Privacy	19
2.1 – Cách mã hoá WEP	19
2.2 – Cách giải mã WEP	21
2.3 – WEP RC4	22
2.4 – Phương thức xác thực WEP	23
2.5 – Việc quản lý khoá mã	26
2.6 – Điểm yếu của WEP	27
3 – Các phương thức tấn công mạng không dây	28
3.1 – Tấn công WEP	29
3.2 – Tấn công SSID	33
3.3 – Kỹ thuật nghe lén	35
3.4 – Tấn công từ chối dịch vụ DoS	38
3.5 – War driving	39
3.6 – Tấn công qua cổng hậu (back door)	40

CHƯƠNG 3 – CÁC GIẢI PHÁP BẢO VỆ MẠNG KHÔNG DÂY	43
1 – Các giải pháp truyền thống	43
1.1 – Các chính sách bảo mật	43
1.2 – Tăng cường nhận thức của người dùng	46
2 – Các giải pháp bảo mật cơ bản	46
2.1 – Máy chủ cung cấp dịch vụ chứng thực từ xa RADIUS	46
2.2 – Lọc địa chỉ MAC	47
2.3 – Thiết lập SSID	49
2.4 – Lựa chọn ăng ten	50
2.5 – Mạng LAN ảo	51
3 – Bảo mật truy cập không dây WPA	51
3.1 – Các đặc tính của TKIP và Michael	52
3.2 – Các khoá thời gian TK	54
3.3 – Tiến trình mã hoá và giải mã WPA	56
4 – Chuẩn bảo mật WPA2 (hay 802.11i)	59
4.1 – Khung tin 802.11i	60
4.2 – Điểm yếu của 802.11i	61
5 – Thiết lập cơ chế chứng thực người dùng	62
5.1 – Giao thức chứng thực có thể mở rộng EAP	63
5.2 – Khung 802.1x	64
5.3 – Cơ chế chứng thực 802.1x	65
5.4 – Các phương thức chứng thực EAP	69
6 – Bảo mật mạng không dây với mạng riêng ảo	75
6.1 – Mạng riêng ảo VPN làm việc như thế nào ?	76
6.2 – Quản lý công nghệ VPN	77
6.3 – Các giao thức của VPN	78
7 – Hệ thống nhận dạng xâm nhập mạng không dây IDS	83

7.1 – Nhận dạng xâm nhập	83
7.2 – Hệ thống phát hiện xâm nhập không dây	84
7.3 – Kiến trúc IDS	84
7.4 – Dò tìm vị trí vật lý	85
7.5 – Thúc đẩy việc thi hành các chính sách	86
7.6 – Phát hiện nguy hiểm	86
7.7 – Các hạn chế của IDS không dây	88
7.8 – Kết luận	89
KẾT LUẬN	90
TÀI LIỆU THAM KHẢO	92

