

**ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN**

PHẠM HỒNG VIỆT

**MỘT SỐ VẤN ĐỀ AN NINH
TRONG MẠNG MÁY TÍNH KHÔNG DÂY**

LUẬN VĂN THẠC SĨ

THÁI NGUYÊN - 2009

**ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN**

PHẠM HỒNG VIỆT

**MỘT SỐ VẤN ĐỀ AN NINH
TRONG MẠNG MÁY TÍNH KHÔNG DÂY**

Chuyên Ngành: Khoa Học Máy Tính
Mã số: 604801

LUẬN VĂN THẠC SĨ

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. NGUYỄN GIA HIỂU

THÁI NGUYỄN - 2009

MỤC LỤC

	Trang
DANH MỤC CHỮ VIẾT TẮT	i
DANH MỤC HÌNH VẼ	ii
LỜI CẢM ƠN	iii
MỞ ĐẦU	1
CHƯƠNG I. TỔNG QUAN VỀ MẠNG KHÔNG DÂY	2
I. GIỚI THIỆU CHUNG	2
1. Giới thiệu	2
2. Quá trình phát triển	4
II. CÔNG NGHỆ CHO MẠNG KHÔNG DÂY	5
1. Công nghệ trải phổ	5
1.1 Công nghệ trải phổ trực tiếp	6
1.2 Công nghệ trải phổ nhảy tần	8
1.3 OFDM- Ghép kênh phân chia theo tần số trực giao	10
2. Một số thành phần kỹ thuật khác	11
2.1 Đa truy cập cảm ứng sóng mang – Tránh xung đột CSMA/CA	11
2.2 Yêu cầu và sẵn sàng gửi RTS/CTS	12
III. MÔ HÌNH HOẠT ĐỘNG CỦA MẠNG KHÔNG DÂY	13
1. Phương thức Adhoc WLAN (IBSS)	13
2. Phương thức InFraStructure (BSS)	14
3. Mô hình mạng diện rộng (WiMax)	16
IV. CÁC CHUẨN CỦA MẠNG KHÔNG DÂY	16
1. Chuẩn 802.11.WLAN	16
1.1 IEEE 802.11	17

1.2 IEEE 802.11b	17
1.3 IEEE 802.11a	19
1.4 IEEE 802.11g	20
1.5 IEEE 802.11e	21
2. Chuẩn 802.16.Broadband wireless	22
3. Chuẩn 802.15.Bluetooth	22
V. BẢO MẬT TRONG MẠNG KHÔNG DÂY	22
1. Bảo mật với WEP	22
2. Bảo mật với TKIP	23
CHƯƠNG II . AN NINH TRONG MẠNG KHÔNG DÂY	24
I. VẤN ĐỀ AN NINH TRONG MẠNG KHÔNG DÂY	24
II. CÁC LOẠI HÌNH TẤN CÔNG MẠNG KHÔNG DÂY	25
1. Tấn công bị động - Passive attacks	25
1.1 Định nghĩa	25
1.2 Phương thức bắt gói tin (Sniffing)	25
2. Tấn công chủ động - Active attacks	27
2.1 Định nghĩa	27
2.2 Mạo danh, truy cập trái phép	27
2.3 Sửa đổi thông tin	28
2.4 Tấn công từ chối dịch vụ (DOS)	28
3. Tấn công kiểu chèn ép - Jamming attacks	30
4. Tấn công theo kiểu thu hút - Man in the middle attacks	30
III. GIẢI PHÁP KHẮC PHỤC	31
1. Quy trình xây dựng hệ thống thông tin an toàn	31
1.1 Đánh giá và lập kế hoạch	31
1.2 Phân tích hệ thống và thiết kế	31
1.3 Áp dụng vào thực tế	31

1.4 Duy trì và bảo dưỡng	32
2. Các biện pháp và công cụ bảo mật hệ thống	32
2.1. Các biện pháp	32
2.1.1 Kiểm soát truy nhập	32
2.1.2 Kiểm soát sự xác thực người dùng (Authentication)	32
2.1.3 Tăng cường nhận thức người dùng	33
2.2. Các công cụ bảo mật hệ thống	33
2.2.1. Chứng thực bằng địa chỉ MAC	33
2.2.2. Chứng thực bằng SSID	35
2.2.3. Chữ ký điện tử	36
2.3. Mã hóa dữ liệu	37
2.3.1. Sử dụng hệ mật mã DES	37
2.3.2. Sử dụng hệ mật mã RSA	38
2.4. Phương thức chứng thực và mã hóa WEP	39
2.4.1. Phương thức chứng thực	40
2.4.2. Cách mã hoá WEP	42
2.4.3. Cách giải mã WEP	44
2.4.4. Quản lý mã khoá	45
2.4.5. Các ưu nhược điểm của WEP	46
2.5. Giao thức bảo toàn dữ liệu với khoá theo thời gian TKIP	47
2.5.1. Bảo mật với TKIP	47
IV. CHUẨN XÁC THỰC	50
1. Nguyên lý RADIUS Server	50
2. Phương thức chứng thực mở rộng EAP	52
2.1. Bản tin EAP	53
2.2. Các bản tin yêu cầu và trả lời EAP	53
2.2.1. Loại code 1: Identity	54
2.2.2. Loại code 2: Notification (Thông báo)	54
2.2.3. Loại code 3: NAK	55

2.2.4. Loại code 4: Chuỗi MD5 (MD5 Challenge)	55
2.2.5. Loại code 5: One - time password (OPT)	55
2.2.6. Loại code 6: Đặc điểm thẻ Token	55
2.2.7. Loại code 13: TLS	56
2.2.8. Các loại mã khác	56
2.3. Các khung trong EAP	56
2.4. Chứng thực công	57
2.5. Kiến trúc và thuật ngữ trong chứng thực EAP	57
2.6. Dạng khung và cách đánh địa chỉ của EAPOL	58
2.6.1. Dạng khung	58
2.6.2. Đánh địa chỉ	59
2.7. Một ví dụ về trao đổi thông tin trong chứng thực EAP	60
CHƯƠNG III . ỨNG DỤNG THỰC TẾ MẠNG KHÔNG DÂY TẠI TRƯỜNG ĐHKTCN.	62
I. MÔ HÌNH MẠNG KHÔNG DÂY TRONG TRƯỜNG ĐHKTCN	62
1. Mô hình logic và sơ đồ phủ sóng vật lý tổng thể tại trường	63
1.1. Mô hình thiết kế logic	63
1.2. Sơ đồ phủ sóng vật lý tổng thể tại trường	64
2. Thiết kế chi tiết của hệ thống	65
2.1. Mô hình thiết kế chi tiết hệ thống mạng không dây	65
2.2. Thiết bị sử dụng trong hệ thống mạng không dây	66
2.3. Phân bổ thiết bị sử dụng trong hệ thống	72
II. GIẢI PHÁP BẢO MẬT TRONG MẠNG KHÔNG DÂY TẠI ĐHKTCN	72
1. Yêu cầu bảo vệ thông tin	73
2. Các bước thực thi an toàn bảo mật cho hệ thống	75
III. CHƯƠNG TRÌNH THỰC TẾ ĐÃ XÂY DỰNG	77
1. Điều khiển các AP thông qua Wireless controler	78

2. Chính sách và công cụ bảo mật áp dụng cho hệ thống	79
IV. ĐÁNH GIÁ KẾT QUẢ	84
KẾT LUẬN	86
TÀI LIỆU THAM KHẢO	88

DANH MỤC CHỮ VIẾT TẮT

AIS	Automated Information System
AP	Access Point
ASCII	American Standard Code for Information Interchange
BSS	Basic Service Set
CRC-32	Cyclic Redundancy Check-32
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
DoS	Denial-of-Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
FHSS	Frequency Hopping Spread Spectrum
FMS	Fluhrer, Mantin và Shamir
I&A	Identification & Authentication
ICV	Integrity Check Value
IDS	Intrusion-Detection System
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
IV	Initialization vector
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MIC	Message Integrity Check
MSDU	MAC Service Data Unit
PEAP	Protected Extensible Authentication Protocol

PED	Personal Electronic Device
PMK	Pairwise Master Key
PRNG	Pseudo-Random Number Generator
RADIUS	Remote Authentication Dial In Service
RC4	Rivest Code 4
SKA	Shared Key Authentication
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access
OFDM	Orthogonal Frequency Division Multiplex
ACK	Acknowledgement
RTS/CTS	Request To Send/Clear To Sen
IBSS	Independent Basic Service Sets
BSS	Basic service sets
ISM	Industrial, Scientific, Medical
PSK	Phase Shift Keying
CCK	Complementary Code Keying
FCC	Federal Communications Commission
LOS	Light of Sight
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access Control System
DES	Data Encryption Standard

IDEA	International Data Encryption Algorithm
AES	Advanced Encryption Standard
RSA	Rivest, Shamir, Adleman
TLS	Transport Layer Security
EAPOW	EAP Over Wireless

DANH MỤC HÌNH VẼ

- Hình 1: Độ nhiễu của tần số
- Hình 2: Sự mã hoá thông tin của trải phổ chuỗi trực tiếp
- Hình 3: Chuyển đổi tần số trên các kênh
- Hình 4: Quá trình gửi RTS/CTS
- Hình 5: Mô hình mạng Adhoc
- Hình 6: Mô hình kết nối tập dịch vụ cơ bản BSS
- Hình 7: Mô hình mạng diện rộng Wimax
- Hình 8: Phân bố băng tần ISM
- Hình 9: Mô tả quá trình chứng thực bằng địa chỉ MAC
- Hình 10: Mô tả quá trình chứng thực bằng SSID
- Hình 11: Quá trình ký trong message
- Hình 12: Quá trình mã hoá sử dụng hệ mật mã DES
- Hình 13: Quá trình mã hoá sử dụng hệ mật mã RSA
- Hình 14: Mô tả quá trình chứng thực giữa Client và AP
- Hình 15: Thuật toán mã hóa WEP
- Hình 16: Quá trình giải mã WEP
- Hình 17: Quá trình bảo mật dùng TKIP
- Hình 18: Mô hình chứng thực sử dụng RADIUS Server
- Hình 19: Quá trình chứng thực RADIUS Server
- Hình 20: Kiến trúc EAP cơ bản
- Hình 21: Cấu trúc khung của bản tin yêu cầu và trả lời
- Hình 22: Cấu trúc các khung EAP thành công và không thành công
- Hình 23: Cấu trúc cổng

- Hình 24: Cấu trúc cơ bản của khung EAPOL
- Hình 25: Quá trình chứng thực EAP
- Hình 26: Mô hình logic mạng không dây tại trường
- Hình 27: Mô hình phủ sóng tại trường
- Hình 28: Sơ đồ phân bố các Access point
- Hình 29: Giao diện quản trị của WLAN Controller 4420
- Hình 30: Hệ thống 10 AP được quản lý
- Hình 31: Các mức truy cập của hệ thống
- Hình 32: Các chính sách truy cập của USERS_GV_ACL
- Hình 33: Các chính sách truy cập của GUEST_ACL
- Hình 34: Bảo mật lớp 2 của WLAN SSID: Quản trị mạng dhkten
- Hình 35: Bảo mật lớp 3 của WLAN SSID: Quản trị mạng dhkten
- Hình 36: Bảo mật của WLAN SSID: Sinh viên dhkten và Khách
- Hình 37: Bảo mật của WLAN SSID: Cán bộ và Giảng viên dhkten
- Hình 38: Tạo ra các users chứng thực Web Authentication
- Hình 39: Cấu hình chức năng bảo mật Web Authentication
- Hình 40: Đăng nhập trong chính sách Web Authentication
- Hình 41: Bảng MAC Address Table để chứng thực và quản lý