ĐẠI HỌC THÁI NGUYÊN

KHOA CÔNG NGHỆ THÔNG TIN

VŨ ANH TUẤN

GIẢI PHÁP NÂNG CAO ĐỘ AN NINH THÔNG TIN TRONG MẠNG LAN KHÔNG DÂY CHUẨN IEEE 802.11i

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2009

ĐẠI HỌC THÁI NGUYÊN

KHOA CÔNG NGHỆ THÔNG TIN

VŨ ANH TUẤN

GIẢI PHÁP NÂNG CAO ĐỘ AN NINH THÔNG TIN TRONG MẠNG LAN KHÔNG DÂY CHUẨN IEEE 802.11i

Nghành: Khoa học máy tính

Mã số: 60.48.01

LUẬN VĂN THẠC SĨ

Người hướng dẫn khoa học:

PGS.TS NGUYỄN VĂN TAM

Thái Nguyên - 2009

DANH MỤC CÁC TỪ, KÝ HIỆU VIẾT TẮT

AAA	Authentication Authorization Audit
AES	Advanced Encryption Standard
AP	Access point
BSS	Basic Service Set
CA	Certificate Authority
CCK	Complimentary Code Keying
CDMA	Code Division Multiple Access
CMSA/CD	Carrier Sense Multiple Access with Collision Detection
CRC	Cyclic redundancy check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DOS	Denial of service
DRDOS	Distributed Reflection DOS
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EAPOW	EAP Over Wireless
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
GPS	Global Positioning System
ICMP	Internet Control Message Protocol
ICV	Intergrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IV	Initialization Vector

LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Network
MIC	Message Integrity Check
OFDM	Orthogonal Frequency Division
OSI	Open Systems Interconnection
PAN	Person Area Network
PDA	Personal Digital Assistant
PEAP	Protected EAP Protocol
PKI	Public Key Infrastructure
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RFC	Request For Comment
RTS	Request To Send
SSID	Service Set ID
SSL	Secure Sockets Layer
SWAP	Standard Wireless Access Protocol
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPC	Transmission Power Control
UDP	User Datagram Protocol
UNII	Unlicensed National Information Infrastructure
VLAN	Virtual LAN
WAN	Wide Area Network
WEP	Wired Equivalent Protocol
WLAN	Wireless LAN
WPA	Wi-fi Protected Access

MỤC LỤC

Trang phụ bìa
Lời cam đoan .....
Mục lục i
Danh mục các ký hiệu, các chữ viết tắt iv
Danh mục các hình (hình vẽ, ảnh chụp, đồ thị...) vi
MỞ ĐẦU 1
1. Nền tảng và mục đích 1
2. Cấu trúc của luận văn 2
CHƯƠNG 1: TỔNG QUAN VỀ MẠNG LAN KHÔNG DÂY CHUẨN IEEE 802.11 3
1.1 Giới thiệu 3
1.1.1 Ưu điểm của mạng máy tính không dây 3
1.1.2 Hoạt động của mạng máy tính không dây 4
1.1.3 Các mô hình của mạng máy tính không dây cơ bản 5
1.2 Kiến trúc mạng LAN chuẩn IEEE 802.11 6
1.2.1 Tầng vật lý mạng LAN không dây 6
1.2.2 Tầng điều khiển truy nhập CSMA/CA 9
1.3 Các chuẩn của 802.11 10
1.3.1 Nhóm lớp vật lý PHY 11
1.3.2 Nhóm lớp liên kết dữ liệu MAC 12
1.4. Các kiến trúc cơ bản của chuẩn 802.11 13
1.4.1 Trạm thu phát - STA 13
1.4.2 Điểm truy cập - AP 14
1.4.3 Trạm phục vụ cơ bản - BSS 14
1.4.4 BSS độc lập - IBSS 15
1.4.5 Hệ thống phân tán - DS 15
1.4.6 Hệ thống phục vụ mở rộng - ESS 15
1.4.7 Mô hình thực tế 16
CHƯƠNG 2: AN NINH MẠNG LAN KHÔNG DÂY 17
2.1 Các kiểu tấn công đối với mạng không dây 17
2.1.1 Tấn công bị động - Passive attacks 17
2.1.2 Tấn công chủ động - Active attacks 19

2.1.2.1 Mạo danh, truy cập trái phép 20
2.1.2.2 Tấn công từ chối dịch vụ - DOS 21
2.1.2.3 Tấn công cưỡng đoạt điều khiển và sửa đổi thông tin - Hijacking and Modification 23
2.1.2.4 Dò mật khẩu bằng từ điển - Dictionary Attack 25
2.1.3 Tấn công kiểu chèn ép - Jamming attacks 26
2.1.4 Tấn công theo kiểu thu hút - Man in the middle attacks 26
2.2 An ninh mạng máy tính không dây 27
2.2.1 Giải pháp an ninh WEP 28
2.2.2.1 Phương thức chứng thực 28
2.2.2.2 Phương thức mã hóa 29
2.2.2.3 Các ưu, nhược điểm của WEP 32
2.2.2 Giải pháp an ninh WPA, WPA2 34
2.2.1.1 WPA - Wi-fi Protected Access 34
2.2.2.2 WPA2 - Wi-fi Protected Access 2 35
CHƯƠNG 3: AN NINH MẠNG LAN KHÔNG DÂY CHUẨN 802.11i.... 36
3.1 Tổng quan về chuẩn IEEE 802.11i 36
3.1.1 TKIP 36
3.1.1.1 Khác biệt giữa TKIP và WEP 36
3.1.1.2 Véc tơ khởi tạo 39
3.1.1.3 Quá trình trộn khóa 39
3.1.1.4 Mã kiểm tra toàn vẹn Michael 40
3.1.2 CCMP 41
3.1.2.1 Chế độ đếm kết hợp CBC-MAC 41
3.1.2.2 Quá tình hoạt động của CCMP 43
3.1.3 802.1x 37
3.1.3.1 Nguyên lý RADIUS Server 45
3.1.3.2 Giao thức chứng thực mở rộng EAP 47
3.2 Thuật toán mã hoá sử dụng trong chuẩn IEEE 802.11i 57
3.2.1 Giới thiệu 57
3.2.2 Mô tả thuật toán 57
3.2.3 Tối ưu hóa 61
3.2.4 Khả năng an toàn 61
3.2.5 Kết luận 61

3.3 Triển khai an ninh mạng LAN không dây trên nền chuẩn 802.11i 63
3.3.1 Mô tả bài toán 63
3.3.2 Thiết kế sơ đồ mạng 63
3.3.3. Cấu hình bảo mật 63
3.3.4 Thử nghiệm an ninh. 66
KẾT LUẬN 67
TÀI LIỆU THAM KHẢO 68

MỞ ĐẦU

1. Nền tảng và mục đích

Khi thiết kế các yêu cầu kỹ thuật cho mạng không dây, chuẩn 802.11 của IEEE đã có tính đến vấn đề bảo mật dữ liệu đường truyền qua phương thức mã hóa. Trong đó, phương thức WEP đã được đa số các nhà sản xuất thiết bị không dây hỗ trợ như là một phương thức mặc định bảo mật không dây. Tuy nhiên, những phát hiện gần đây về điểm yếu của chuẩn 802.11 WEP cho thấy WEP không phải là một cơ chế bảo mật toàn diện cho mạng WLAN.

Giải pháp khác được Wi-Fi Alliance đưa ra gọi là Wi-Fi Protected Access (WPA). Một trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP (Temporal Key Integrity Protocol). WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu. Tuy nhiên, WPA cũng không hỗ trợ các thiết bị cầm tay và máy quét mã vạch. Điều này cũng có nghĩa rằng kĩ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất.

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2. WPA2 là thế hệ thứ hai của WPA, nó có thể tương thích ngược với các sản phẩm hỗ trợ WPA. Kiểu mã hoá bảo mật WPA2 sử dụng thuật toán mã hoá mạnh mẽ được gọi là Chuẩn mã hoá nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Sự chuyển đổi sang 802.11i và mã hoá AES được xem như là bảo mật tốt hơn nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard).

Mục đích của đề tài là tìm hiểu chung về an ninh chuẩn IEEE 802.11, Giải pháp sử dụng chuẩn mật mã AES bảo đảm tính mật và tính toàn vẹn khung tin trong WLAN.

2. Cấu trúc của luận văn

Ngoài phần mở đầu và kết luận, nội dung của luận văn này được bố cục như sau:

Chương 1: Trình bày tổng quan về mạng LAN không dây chuẩn 802.11i.

Chương 2: Trình bày về an ninh mạng LAN không dây, các kiểu tấn công và an ninh đối với mạng LAN không dây.

Chương 3: An ninh mạng LAN không dây chuẩn 802.11i, trình bày thuật toán mã hóa sử dụng trong chuẩn IEEE 802.11i và triển khai.

Cuối cùng là tài liệu tham khảo.

CHƯƠNG I:
TỔNG QUAN VỀ MẠNG LAN KHÔNG DÂY CHUẨN IEEE 802.11

1.1 Giới thiệu

Thuật ngữ "mạng máy tính không dây" nói đến công nghệ cho phép hai hay nhiều máy tính giao tiếp với nhau dùng những giao thức mạng chuẩn nhưng không cần dây cáp mạng. Nó là một hệ thống mạng dữ liệu linh hoạt được thực hiện như một sự mở rộng hoặc một sự lựa chọn mới cho mạng máy tính hữu tuyến (hay còn gọi là mạng có dây). Các mạng máy tính không dây sử dụng các sóng điện từ không gian (sóng vô tuyến hoặc sóng ánh sáng) thu, phát dữ liệu qua không khí, giảm thiểu nhu cầu về kết nối bằng dây. Vì vậy, các mạng máy tính không dây kết hợp liên kết dữ liệu với tính di động của người sử dụng.

Công nghệ này bắt nguồn từ một số chuẩn công nghiệp như là IEEE 802.11 đã tạo ra một số các giải pháp không dây có tính khả thi trong kinh doanh, công nghệ chế tạo, các trường đại học… khi mà ở đó mạng hữu tuyến là không thể thực hiện được. Ngày nay, các mạng máy tính không dây càng trở nên quen thuộc hơn, được công nhận như một sự lựa chọn kết nối đa năng cho một phạm vi lớn các khách hàng kinh doanh.

1.1.1 Ưu điểm của mạng máy tính không dây

Mạng máy tính không dây đang nhanh chóng trở thành một mạng cốt lõi trong các mạng máy tính và đang phát triển vượt trội. Với công nghệ này, những người sử dụng có thể truy cập thông tin dùng chung mà không phải tìm kiếm chỗ để nối dây mạng, chúng ta có thể mở rộng phạm vi mạng mà không cần lắp đặt hoặc di chuyển dây. Các mạng máy tính không dây có ưu điểm về hiệu suất, sự thuận lợi, cụ thể như sau: