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

BÙI PHI LONG

NGHIÊN CỨU VẤN ĐỀ AN NINH MẠNG INTERNET KHÔNG DÂY VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2009

ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN

……..*……..

BÙI PHI LONG

NGHIÊN CỨU VẤN ĐỀ AN NINH MẠNG INTERNET KHÔNG DÂY VÀ ỨNG DỤNG

***Chuyên nghành*: KHOA HỌC MÁY TÍNH**
***Mã số* : 60.48.01**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

***Người hướng dẫn khoa học*: PGS.TS NGUYỄN VĂN TAM**

THÁI NGUYÊN - 2009

MỤC LỤC

Trang

TRANG PHỤ BÌA…….

LỜI CÁM ƠN……...…….

LỜI CAM ĐOAN...……..

MỤC LỤC…….i

DANH MỤC CÁC KÝ HIỆU, CHỮ CÁI VIẾT TẮT…….……..…..v

DANH MỤC CÁC BẢNG…….……..…...…ix

DANH MỤC CÁC HÌNH…….……..……x

MỞ ĐẦU……...1

CHƯƠNG 1. TỔNG QUAN VỀ MẠNG INTERNET……....3

1.1. Giới thiệu công nghệ mạng Internet không dây và ứng dụng …….……..3

1.1.1. Công nghệ mạng Internet không dây……3

1.1.2. Ưu và nhược điểm của công nghệ mạng Internet không dây……....4

1.1.2.1. Ưu điểm.…….……..4

1.1.2.2. Nhược điểm…….5

1.2. Kiến trúc cơ bản của mạng LAN không dây…….5

1.2.1. Giới thiệu chung về mạng LAN không dây – WLAN……...5

1.2.2. Chuẩn 802.11 ……6

1.2.2.1. Nhóm lớp vật lý PHY bao gồm các chuẩn:…….……7

1.2.2.2. Nhóm lớp liên kết dữ liệu MAC bao gồm các chuẩn:…….8

1.2.3. Các mô hình WLAN (chuẩn 802.11)…….9

1.2.3.1. Trạm thu phát – STA…….. 9

1.2.3.2. Điểm truy cập – AP…… 9

1.2.3.3. Mạng 802.11 linh hoạt về thiết kế, gồm 3……..…… 10

1.2.3.4. WEP – Wired Equivalent Privacy ……... 14
1.2.3.5. WEP key lengths ……..14
1.2.3.6. WPA – Wi- fi Protected Access ……...15
1.2.3.7. WPA2 – Wi- fi Protected Access 2 ……..…. 15
1.3. Kiến trúc cơ bản của mạng WAN không dây……..16
1.3.1. Thế hệ thứ 1 (1G) …….…….. 17
1.3.2. Thế hệ thứ 2 (2G) ……17
1.3.3. Thế hệ di động thứ 3 (3G)……... 18
1.4. Kiến trúc cơ bản của Internet không dây…….22
1.4.1. Kiến trúc cơ bản của Internet không dây – chuẩn WAP…….22
1.4.1.1. Sơ bộ về WAP……..……..22
1.4.1.2. Các mô hình giao tiếp trên WAP ……..24
1.4.1.3. Ưu và nhược điểm của WAP ……28
1.4.1.4. Các thành phần của WAP…… 30
1.4.2. Kiến trúc cơ bản của mạng WPAN không dây……..…… 37
1.4.3. Kiến trúc cơ bản của mạng WMAN không dây ……..49
1.4.3.1. Đặc điểm nổi bật của WiMAX di động ……40
1.4.3.2. Mô hình ứng dụng WiMAX……..40
1.4.4. Mạng không dây WRAN……42
1.5. Tổng kết……...42
CHƯƠNG 2. TỔNG QUAN VỀ AN NINH MẠNG INTERNET KHÔNG DÂY …..44

2.1. Một số kỹ thuật tấn công Internet không dây.....44
2.1.1. Tấn công bị động – Passive attacks……44
2.1.1.1. Định nghĩa……44
2.1.1.2. Kiểu tấn công bị động cụ thể - Phương thức bắt gói tin (Sniffing)…...45
2.1.2. Tấn công chủ động – Active attacks……47
2.1.2.1. Định nghĩa……47
2.1.2.2. Các kiểu tấn công chủ động cụ thể……..48
2.1.3. Tấn công kiểu chèn ép - Jamming attacks ……54
2.1.4. Tấn công theo kiểu thu hút - Man in the middle attacks……. 55
2.1.5. Tấn công vào các yếu tố con người …….……55
2.1.6. Một số kiểu tấn công khác ……...…56
2.2. Giải pháp an ninh cho mạng Internet không dây (WAP)…….…57
2.2.1. Vấn đề bảo mật trên WAP……..57
2.2.1.1. So sánh các mô hình bảo mật……57
2.2.1.2. WAP Gateway……..63
2.2.1.3. TLS và WTLS……...66
2.3. Tổng kết ……..…….……68
CHƯƠNG 3: MẠNG INTERNET KHÔNG DÂY VÀ THỬ NGHIỆM ……70
3.1. Thiết kế mô hình mạng Internet không dây trong trường Việt Đức TN…….70
3.1.1. Nguyên tắc thiết kế……70
3.1.2. Mô hình logic và sơ đồ phủ sóng vật lý tổng thể tại trường……...71
3.1.2.1. Mô hình thiết kế logic……...71
3.1.1.2. Sơ đồ phủ sóng vật lý tổng thể tại trường……...71
3.1.3. Thiết kế chi tiết của hệ thống……..73
3.1.3.1. Mô hình thiết kế chi tiết hệ thống mạng không dây……...…73
3.1.3.2. Thiết bị sử dụng trong hệ thống mạng không dây…….……73
3.1.3.3. Phân bổ thiết bị sử dụng trong hệ thống……75

3.2. Giải pháp bảo mật trong mạng không dây tại CĐCN Việt Đức Thái Nguyên …..75
3.2.1. Yêu cầu bảo vệ thông tin……...76
3.2.1.1. Bảo vệ dữ liệu:……77
3.2.1.2. Bảo vệ các tài nguyên sử dụng trên mạng:……77
3.2.1.3. Bảo vệ danh tiếng cơ quan:……78
3.2.2. Các bước thực thi an toàn bảo mật cho hệ thống……..78
3.2.2.1. Các hoạt động bảo mật ở mức một……78
3.2.2.2. Các hoạt động bảo mật ở mức hai……..79
3.3. Chương trình thực tế đã xây dựng……...79
3.4. Đánh giá kết quả……..80
3.5. Một số hướng dẫn để bảo vệ máy tính an toàn khi dùng Internet không dây…….80
3.5.1. Tối ưu hóa Wi-Fi cho các VoIP, Video Game……80
3.5.2. Ưu tiên hóa tải gói dữ liệu…….….. 81
3.5.3. Tắt Wi-Fi khi không dùng đến ……83
3.5.4. Theo dõi những người không mời mà đến trên mạng Wi-Fi của bạn……..83
3.5.5. Loại bỏ điểm kết nối không dây an toàn…… 84
3.5.6. Vô hiệu hóa Peer-to-Peer Wi-Fi ……85
3.6. Tấn công Website – Cách xử lý……..…….…….87
3.7. Tổng kết……...……..88
KẾT LUẬN ……...90
TÀI LIỆU THAM KHẢO……..92
PHỤ LỤC……...94

DANH MỤC CÁC KÝ HIỆU, CHỮ CÁI VIẾT TẮT

AAA - Authentication Authorization Audit

ACL - Access control lists

ACS - Access Control Server

ACU - Aironet Client Utility

AES – Advanced Encryption Standard

AP - Access point

APOP - Authentication POP

BSS - Basic Service Set

BSSID - Basic Service Set Identifier

CA - Certificate Authority

CCK - Complimentary Code Keying

CDMA - Code Division Multiple Access

CHAP - Challenge Handshake Authentication Protocol

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

DMZ - Demilitarized Zone

DOS - Denial of service

DRDOS - Distributed Reflection DOS

DS - Distribution System

DSSS - Direct Sequence Spread Spectrum

EAP - Extensible Authentication Protocol

EAPOL - EAP Over LAN

EAPOW - EAP Over Wireless

ESS - Extended Service Set

ETSI - European Telecommunications Standards Institute

FCC - Federal Communications Commissio

FHSS – Frequency Hopping Spread Spectrum

GPS - Global Positioning System

HiperLAN - High Performance Radio LAN

HTML -HyperText Markup Language

HTTP - HyperText Transfer Protocol

IBSS - Independent Basic Service Set

ICMP -Internet Control Message Protocol

ICV – Intergrity Check Value

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IR - Infrared Light

IKE - Internet Key Exchange

IP - Internet Protocol

IPSec - Internet Protocol Security

IrDA - Infrared Data Association

ISDN -Integrated Services Digital Network

ISM - Industrial Scientific and Medical

ISP - Internet Service Provider

ITU - International Telecommunication Union

IV - Initialization Vector

LAN - Local Area Network

LCP – Link Control Protocol

LEAP - Light Extensible Authentication Protocol

LLC - Logical Link Control

LOS - Light of Sight

MAC - Media Access Control

MAN - Metropolitan Area Network

MIC - Message Integrity Check

MSDU - Media Access Control Service Data Unit

OCB - Offset Code Book

OFDM - Orthogonal Frequency Division

OSI - Open Systems Interconnection

OTP - One-time password

PAN - Person Area Network

PBCC - Packet Binary Convolutional Coding

PCMCIA - Personal Computer Memory Card International Association

PDA - Personal Digital Assistant

PEAP - Protected EAP Protocol

PKI-Public Key Infrastructure

PRNG - Pseudo Random Number Generator

QoS - Quality of Service

RADIUS - Remote Access Dial-In User Service

RF - Radio frequency

RFC - Request For Comment

RTS - Request To Send

SIG - Special Interest Group

SSH - Secure Shell

SSID - Service Set ID

SSL - Secure Sockets Layer

STA - Station

SWAP - Standard Wireless Access Protocol

TACACS - Terminal Access Controller Access Control System

TCP - Transmission Control Protocol

TFTP - Trivial File Transfer Protocol

TKPI - Temporal Key Integrity Protocol

TLS - Transport Layer Security

TPC - Transmission Power Control

UDP - User Datagram Protocol

UWB – Ultra Wide Band

UNII - Unlicensed National Information Infrastructure

VLAN - Virtual LAN

WAN - Wide Area Network

WECA - Wireless Ethernet Compatibility

WEP - Wired Equivalent Protocol

Wi-Fi - Wireless fidelity

WLAN - Wireless LAN

WPAN - Wireless Personal Area Network