Computer Science

Christian Wimmer

Wireless LAN Security in a SOHO Environment: A Holistic Approach

Bachelor Thesis

Examicus

YOUR KNOWLEDGE HAS VALUE

- We will publish your bachelor's and master's thesis, essays and papers
- Your own eBook and book - sold worldwide in all relevant shops
- Earn money with each sale

Upload your text at www.GRIN.com
and publish for free

GRIN

Wireless LAN Security in a SOHO Environment: A Holistic Approach

Christian Manfred Wimmer

A project submitted in partial fulfilment of the requirements for the

University of Wales award of B.Sc. (Hons) in Computing & Information Technology,

School of Computing & Communications Technology

North East Wales Institute, Wrexham

May 2006

I. Acknowledgements

I would like to thank my flatmate *Klaus Schedlbauer* for proof reading this paper and for just being there whenever I needed him. Thanks also go to *Jürgen Pörsch* for helping me to start this project and for the idea to study in Newi and to *Nicole Gebert* for inspiring me.

Special thanks go to my project supervisor *John McGinn* who was always there when I needed him and was always helping me, without him this project would not be what it is. Günter Zweck, my stepfather, without his support I would not be where I am now.

Finally I would like to acknowledge *Anton Braun* and *Keshav Srinivasan*, my colleges from overseas, who sacrificed some of their free time to proof-read this paper.

II. Contents

I. ACKNOWLEDGEMENTS **2**

II. CONTENTS **3**

III. LIST OF FIGURES **6**

IV. LIST OF ABBREVIATIONS **7**

V. ABSTRACT **9**

1. INTRODUCTION **10**

2. LITERATURE REVIEW **11**

3. METHODOLOGY **16**

3.1. TIMETABLE AND LOG-KEEPING 17
3.2. THE ARTEFACT 17
3.3. METHODOLOGY REFLECTION 18

4. WLAN BASICS **19**

4.1. THE IEEE STANDARDS 19
4.2. RELATIONSHIP BETWEEN THE WI-FI ALLIANCE AND THE IEEE 21
4.3. WLAN ARCHITECTURE 22
4.3.1. Independent / Ad-Hoc *23*
4.3.2. Infrastructure *23*

5. SECURITY **24**

5.1. SECURITY OBJECTIVES 24
5.2. WLAN SECURITY 25
5.3. WEP ARCHITECTURE 27
5.3.1. How WEP works *27*
5.3.2. WEP – why it doesn't work *30*
5.3.3. WEP Summary *31*
5.4. NEW SECURITY: 802.11I AND WPA 32
5.4.1. Temporal Key Integrity Protocol (TKIP) *32*
5.4.2. What is WPA? *33*
5.4.3. Counter Mode with CBC-MAC and Robust Secure Networks *34*
5.4.4. Mixed Mode – Transitional Security Network (TSN) *35*
5.4.5. 802.11i Summary *35*
5.5. INTERIM AND EXTRA SECURITY SOLUTIONS 36
5.5.1. VPN and IPSec *36*
5.5.2. SSL and SSH *36*

5.5.3. Other alternatives 37
5.6. A BAD SECURITY EXAMPLE: NINTENDO DS 38
6. WIRELESS LAN PENETRATION TEST – AN EXPERIMENT 40
6.1. ASSEMBLING THE GEAR 40
6.2. GATHERING BASIC INFORMATION 41
6.3. ATTACKING WEP 41
6.4. GETTING PAST THE MAC FILTER 43
6.5. GETTING NETWORK SETTINGS 43
6.6. CONCLUSION 43
7. PHYSICAL LAYER SECURITY 45
7.1. FREQUENCIES AND THEIR USE 45
7.1.1. 2.4 GHz WLAN technology 45
7.1.2. 5GHz WLAN technology 46
7.1.3. Advantages and Disadvantages of the frequencies 46
7.2. HOW WLAN SIGNAL STRENGTH IS MEASURED 47
7.3. HOW THE SIGNAL IS AFFECTED 48
7.3.1. Straight-Line Losses 48
7.3.2. Interference 49
7.3.3. Practical Test: Microwave ovens versus WLANs 51
7.4. ANTENNAS AND THEIR IRRADIATION PATTERNS 51
7.4.1. Dipole Antennas 51
7.4.2. Directional Antennas 52
7.4.3. Antenna size matters 53
8. EXPERIMENTS 54
8.1. GENERAL ISSUES 54
8.1.1. Hardware and Software Configuration 54
8.1.2. Measuring the WLAN signal strength 54
8.1.3. Windows and Netstumbler 54
8.1.4. Linux and Wavemon 55
8.2. AVOIDING INTERFERENCE 56
8.3. MAKING THE TEST RESULTS COMPARABLE 56
8.4. EXPERIMENTS AND RESULTS 57
8.4.1. Signal loss for obstacles 57
8.4.2. Using a home-made reflector 57
8.4.3. Other means to shield the Access Point 59
8.5. RECOMMENDATIONS FOR PLACING THE ACCESS POINT TO INCREASE SECURITY 60
9. CRITICAL EVALUATION 61
9.1. EVALUATING THE OBJECTIVES 61

9.2. EVALUATING OF THE PROCESS AND PERSONAL REFLECTION 63

10. CONCLUSION 65

11. REFERENCES 66

12. BIBLIOGRAPHY 70

13. APPENDICES 72

A 1. PROJECT ORGANIZATION RELATED 72

A 1.1 PROJECT PROPOSAL 72
A 1.2 PROJECT SPECIFICATION 73
A 1.3 GANT CHART 74
A 1.4 BRAINSTORMING LOG 75
A 1.5 UNREALIZED ARTEFACT IDEAS 76
A 1.6 PROJECT LOGBOOK (DISCONTINUED) 78

A 2. INFORMATION GATHERING RELATED 82

A 2.1 INTERVIEW TRANSCRIPT, TRANSLATED INTO ENGLISH 82
A 2.2 INTERVIEW TRANSCRIPT, ORGINAL VERSION, GERMAN 85
A 2.3 WARWALK THROUGH WREXHAM 88

A 3. PHYSICAL LAYER RELATED 91

A 3.1. 2.4GHZ CHANNELS AND FREQUENCY OVERVIEW 91
A 3.2. 5 GHZ CHANNELS AND FREQUENCY OVERVIEW 92
A 3.3. EZ-12 PARABOLIC REFLECTOR TEMPLATE (ERSKINEAPE, 2005) 94

III. List of figures

Figure 4-1: A typical 802.1X setup 21

Figure 4-2: Relationship of Wi-Fi and IEEE 802.11 22

Figure 4-3: Independent and ad-hoc networks, (adapted from Gast, 2005 p 16) 23

Figure 5-1: The CIA Triad. (adapted from Brunschweiler, 2004, p. 32) 24

Figure 5-2: Open and WEP Authentication 28

Figure 5-3: Generic stream cipher operation (adapted from Gast 2005, p115) 29

Figure 5-4: The Nintendo DS can connect to WEP networks, but lacks WPA support 39

Figure 6-1: Kismet in action. It gives us all the basic information needed to start the hack ... 41

Figure 6-2: WEP cracking with Aircrack. The 128bit WEP key was found in 4 seconds. 42

Figure 6-3: MAC address spoofing under Linux is easy 43

Figure 7-1: DSSS Channels in 2.4GHz spectrum (Vladimirov et al., 2004, p. 62) 45

Figure 7-2 Signal-to-noise ratio and the noise floor (Gast, 2005 p 233) 48

Figure 7-3 Multiple paths 49

Figure 7-4: Wave combination by superposition. Wave 1 and Wave 2 are almost opposite of each other, the net result is almost nothing. (Adapted from Gast, 2005, p. 237) 50

Figure 7-5: Inter-Symbol Interference 50

Figure 7-6 Signal loss while a microwave oven is operating near an access point 51

Figure 7-7: A typical dipole antenna, found on almost every 802.11 b/g Access Point 52

Figure 7-8: Radiation patterns of omnidirectional and directional antennas 52

Figure 8-1: Netstumbler, the swiss knife of Windows WLAN tools 55

Figure 8-2: Wavemon is a great tool for 802.11 signal measuring 56

Figure 8-3: Home made reflectors in action 58

IV. List of abbreviations

AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
BSSID	Basic Service Set ID
CCMP	Counter Mode with CBC-MAC Protocol. AES based protocol 802.11i
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
dBm	decibel (db) in relation to 1 milli-watt (mW)
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
FMS	Fluhrer-Mantin-Shamir. Used to reference a key recovery attack against WEP.
HR/DSSS	High-Rate Direct Sequence Spread Spectrum
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPsec	IP security. Framework of security protocols, often used for VPN
IR	InfraRed
ISO	ternational Organization for Standardization
ISM	Industrial, Scientific, and Medical Bands
IV	Initalization Vector
LAN	Local Area Network
LEAP	Leightweight Extensible Authentication Protocol).
MAC	Medium Access Control
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection, also known as the ISO – OSI modell
PHY	PHYsical Layer
PMK	Pairwise Master Key
PSK	PreShared Key
RADIUS	Remote Authentication Dial In User Service
RC4	Rivest Cipher 4, a streaming cipher devloped by Ron Rivest, RSA labs

RSN	Robust Security Network, part of 802.11i
SNR	Signal to Noise Ratio
SSH	Secure Shell
SSID	Service Set IDentifier
SSL	Secure Socket Layer
SOHO	Small Office / Home Office
TCP	Transmission Control Protocol
TGi	802.11 Task group i
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol. RC4 based protocol introduced in 802.11i
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity
WiMAX	Worldwide Interoperability for Microwave Access, also known as IEEE 802.16
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
WPA2	WPA v2