

Christian Wimmer

Wireless LAN Security in a SOHO Environment

A Holistic Approach

Bibliographic information published by the German National Library:

The German National Library lists this publication in the National Bibliography; detailed bibliographic data are available on the Internet at <http://dnb.dnb.de> .

This book is copyright material and must not be copied, reproduced, transferred, distributed, leased, licensed or publicly performed or used in any way except as specifically permitted in writing by the publishers, as allowed under the terms and conditions under which it was purchased or as strictly permitted by applicable copyright law. Any unauthorized distribution or use of this text may be a direct infringement of the author s and publisher s rights and those responsible may be liable in law accordingly.

Copyright © 2006 Diplomica Verlag GmbH
ISBN: 9783836619233

Christian Wimmer

Wireless LAN Security in a SOHO Environment

A Holistic Approach

Christian Wimmer

Wireless LAN Security in a SOHO Environment *A Holistic Approach*

Christian Wimmer
Wireless LAN Security in a SOHO Environment
A Holistic Approach

ISBN: 978-3-8366-1923-3
Druck Diplomica® Verlag GmbH, Hamburg, 2008
Zugl. University of Wales, Aberystwyth
Ceredigion, Großbritannien, Bachelorarbeit, 2006

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

© Diplomica Verlag GmbH
<http://www.diplom.de>, Hamburg 2008
Printed in Germany

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.	<i>Independent / Ad-Hoc</i>	23
4.3.2.	<i>Infrastructure</i>	23
5.	SECURITY	24
5.1.	SECURITY OBJECTIVES	24
5.2.	WLAN SECURITY	25
5.3.	WEP ARCHITECTURE	27
5.3.1.	<i>How WEP works</i>	27
5.3.2.	<i>WEP – why it doesn’t work</i>	30
5.3.3.	<i>WEP Summary</i>	31
5.4.	NEW SECURITY: 802.11i AND WPA	32
5.4.1.	<i>Temporal Key Integrity Protocol (TKIP)</i>	32
5.4.2.	<i>What is WPA?</i>	33
5.4.3.	<i>Counter Mode with CBC-MAC and Robust Secure Networks</i>	34
5.4.4.	<i>Mixed Mode – Transitional Security Network (TSN)</i>	35
5.4.5.	<i>802.11i Summary</i>	35
5.5.	INTERIM AND EXTRA SECURITY SOLUTIONS	36
5.5.1.	<i>VPN and IPSec</i>	36
5.5.2.	<i>SSL and SSH</i>	36

5.5.3.	<i>Other alternatives</i>	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.	<i>2.4 GHz WLAN technology</i>	45
7.1.2.	<i>5GHz WLAN technology</i>	46
7.1.3.	<i>Advantages and Disadvantages of the frequencies</i>	46
7.2.	HOW WLAN SIGNAL STRENGTH IS MEASURED	47
7.3.	HOW THE SIGNAL IS AFFECTED	48
7.3.1.	<i>Straight-Line Losses</i>	48
7.3.2.	<i>Interference</i>	49
7.3.3.	<i>Practical Test: Microwave ovens versus WLANs</i>	51
7.4.	ANTENNAS AND THEIR IRRADIATION PATTERNS	51
7.4.1.	<i>Dipole Antennas</i>	51
7.4.2.	<i>Directional Antennas</i>	52
7.4.3.	<i>Antenna size matters</i>	53
8.	EXPERIMENTS	54
8.1.	GENERAL ISSUES	54
8.1.1.	<i>Hardware and Software Configuration</i>	54
8.1.2.	<i>Measuring the WLAN signal strength</i>	54
8.1.3.	<i>Windows and Netstumbler</i>	54
8.1.4.	<i>Linux and Wavemon</i>	55
8.2.	AVOIDING INTERFERENCE.....	56
8.3.	MAKING THE TEST RESULTS COMPARABLE	56
8.4.	EXPERIMENTS AND RESULTS	57
8.4.1.	<i>Signal loss for obstacles</i>	57
8.4.2.	<i>Using a home-made reflector</i>	57
8.4.3.	<i>Other means to shield the Access Point</i>	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, ORIGINAL 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