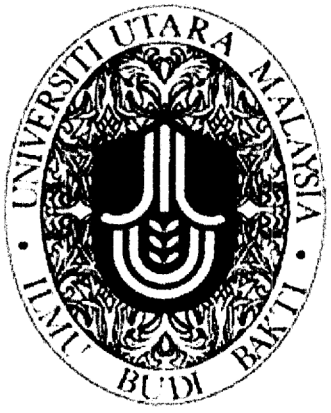
IMPLEMENTING SECURITY IN A CLIENT/SERVER WIRELESS LOCAL AREA NETWORK

CHONG YIN PENG 81950
COURSE:TZ6996



SCHOOL OF INFORMATION TECHNOLOGY

UNIVERSITI UTARA MALAYSIA

2003 - 2004

JABATAN HAL EHWAL AKADEMIK
(*Department of Academic Affairs*)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

CHONG YIN PENG.

calon untuk Ijazah
(candidate for the degree of) **MSc. (INFORMATION TECHNOLOGY)**

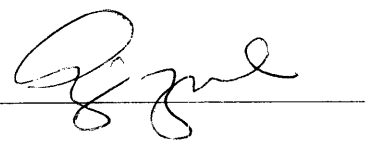
telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

– IMPLEMENTING SECURITY IN A CLIENT/SERVER WIRELESS LOCAL AREA NETWORK.

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the filed is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): PUAN AZIZAH HAJI AHMAD.

Tandatangan
(Signature) : 

Tarikh
(Date) : 23 June 2004

ACKNOWLEGMENTS

Many people supported me during the completion of this thesis with guidance, patience, criticism, helpful assistance and references. This thesis would have never been possible without them. I would like to firstly thank my supervisor Puan Azizah Haji Ahmad for her patience, guidance and encouragement. She was a wonderful supervisor whose assistance and motivation were greatly appreciated. Her diligence in supporting me and accommodation for my visits is highly valuedd.

I would also like to thank the Thesis Committee whom had critically reviewed my proceeding paper and guided me to present my writings and findings in a more procedural and effective way.

I also would like to thank my colleagues back at work for their patience and efforts in sharing their knowledge and skill in WLAN and IT Security to enable me to comprehend the subject more. The time spent to analyze each solution provided is greatly acknowledged.

Last but certainly not least, I would like to show my gratitude to my parents who have been generous with their encouragement throughout.

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a post graduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in her absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or part thereof for financial gain shall not be allowed without written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

LIST OF FIGURES

Page

Figure 2.1: Establishing Man-In-The-Middle Attack by C against A and B by Poisoning ARP Cache 19

Figure 2.2: C executes a Man-In-The-Middle Attack against A and B Undetected 20

Figure 2.3: Scenario illustrating Enterprise Attack on Wired Hosts through a Wireless Vulnerability 22

Figure 2.4: Scenario illustrating Enterprise Attack on Both Wireless Client and Wired Client Through a Wireless Vulnerability 23

Figure 2.5: Scenario illustrating Enterprise Attack on Roaming Wireless Hosts on Different Access Points 24

Figure 2.6: Scenario illustrating Enterprise Attack on Two Wireless Hosts on the Same Access Point 25

Figure 3.1: Initial Insecure Design of WEP-enabled WLAN 37

Figure 4.1: Will there be a slowdown in Wireless Technology Deployment Due to Security? 40

Figure 4.2: Major Pitfall in Deployment 40

Figure 4.3: Biggest Threat to Developing Security In Wireless Network 40

Figure 4.4: Factors that Governs a Secure WLAN 41

Figure 4.5: Final Secure WLAN solution: VPN-IPSec with 802.1X/EAP-TLS enabled WLAN 49

Figure 5.1: Structure of PPTP Packet of User Data 65

Figure 5.2: Structure of an L2TP Packet Of A User Data 65

Figure 5.3: Encryption of an L2TP Packet with IPSec ESP. 66

Figure 5.4: Authentication-Protocol Configuration Option Format for EAP Negotiation 721

Figure 5.5: EAP Packet Format 72
Figure 5.6: EAP Request and Response Packet Format 754
Figure 5.7: An EAP Success and Failure Packet Format 75
Figure 5.8: Content of MD5-Challenge Type-Field 76
Figure 5.9: Wi-Fi Certified Logo 83
Figure 5.10: Different Types of Encryption Achieve Varying Degrees of WLAN Privacy 90
Figure 5.11: Hexadecimal Representation of Bit Patterns 932
Figure 5.12: Indices for Bytes and Bits 93
Figure 5.13: State Array Input and Output 94
Figure 5.14: Key-Block-Round Combinations 97
Figure 5.15: Pseudo Code for the Cipher 98
Figure 5.16: The Effect Of The SubBytes ( ) Transformation On The State. 99
Figure 5.17: SubBytes ( ) Applies the S-Box To Each Byte Of The State. 99
Figure 5.18. S-Box: Substitution Values for the Byte xy (in Hexadecimal Format) 100
Figure 5.19: *ShiftRows ( )* Cyclically Shifts the Last Three Rows In the State.... 101
Figure 5.20: The *MixColumns ( )* Transformation Which Operates On State Column-By-Column 102
Figure 5.21: *AddRoundKey* () XORs each column of the State with a word from the key schedule. 103
Figure 5.22: Pseudo Code for Key Expansion 104
Figure 5.23: Pseudo Code for the Inverse Cipher 105
Figure 5.24: *InvShiftRows* ( ) Cyclically Shifts the Last Three Rows In The State. 105
Figure 5.25: Inverse S-box: Substitution Values for the Bytes xy In Hexadecimal Format. 106
Figure 5.26: Pseudo Code for the Equivalent Inverse Cipher 109

TABLE OF CONTENTS

Page

CERTIFICATION OF THESIS WORK i

ACKNOWLEGMENTS ii

PERMISSION TO USE iii

LIST OF FIGURES iv

ABSTRAK x

ABSTRACT (ENGLISH) xi

CHAPTER ONE:INTRODUCTION 1

1.1 The Context of the Study 1

1.1.1. Netstumbling 4

1.1.2. Network Security Needs Vary from One Consumer to Another 5

1.2 Problem Statement 6

1.3 Research Objective 6

1.4 Significance of the Study 7

CHAPTER TWO: REVIEW OF RELATED LITERATURE 8

2.1. Wired Equavalent Protocol (WEP) 8

2.1.1. IEEE 802.11 Layers 8

2.1.2. WEP in IEEE 802.11 10

2.1.3. Exploiting Key stream Reuse to Read Encrypted Messages 11

2.1.4. Message Authentication 15

2.2. Types Of Local Area Network Attacks 17

2.2.1. Types of Attack: Man-In-The-Middle 18

2.2.2. Mitigation Strategy 25

2.2.2.1. Detection 25

2.2.2.2. Prevention 27

2.2.2.2.1. Access Point Security 27

2.2.2.2.2. Encryption and Authentication plus Possibly a Virtual Private Network 28

2.2.2.2.3. Establishment and Enforcement of Wireless Network Policy ... ...

5.1.4. 802.1X with EAP-TLS 77
5.1.4.1. 802.1X with PEAP 80
5.1.5. Wi-Fi Protected Access (WPA) 81
5.1.6. Wi-Fi Protected Access (WPA) and Temporary Key Integrity Protocol (TKIP) 87
5.1.7. Advanced Encryption Standard (AES) 90
5.1.7.1. Input and Output 91
5.1.7.2. Mathematical Preliminaries of AES Algorithm 95
5.1.7.3. Algorithm Specification 96
5.1.7.3.1. Cipher 97
5.1.7.3.1.1. SubBytes () Transformation 98
5.1.7.3.1.2 ShiftRows ( ) Transformation 100
5.1.7.3.1.3. MixColumns ( ) Transformation 101
5.1.7.3.1.4. AddRoundKey ( ) Transformation 102
5.1.7.3.1.5. Key Expansion 103
5.1.7.3.2. Inverse Cipher 104
5.1.7.3.2.1. InvShiftRows ( ) Transformation 105
5.1.7.3.2.2. InvSubBytes ( ) Transformation 106
5.1.7.3.2.3. InvMixColumns ( ) Transformation 106
5.1.7.3.2.4. Inverse of AddRoundKey ( ) Transformation 107
5.1.7.3.2.5. Equivalent Inverse Cipher 107
5.1.7.4. Implementation Issues 109
5.1.7.4.1. Key Length Requirements 109
5.1.7.4.2. Key Restrictions 109
5.1.7.4.3. Parameterization of Key Length, Block Size and Round Number 109
5.1.7.4.4. Complementary Software/Hardware 110
5.1.7.4.5. Implementation Suggestions regarding Various Platforms 110
5.2. Microsoft Enterprise WLAN Deployment 110

5.2.1. Security Solution: 802.1X for WLAN 111
5.2.2. Infrastructure Solution 114
5.2.3. WLAN Pilot Deployment and Results 118
5.2.4. OTG Key Learning from WLAN Pilot Deployment 119
CHAPTER SIX: CONCLUSION 123
6.1. Technology 1233
6.2. People 125
6.3. Process 125
Reference xi
Appendix xiiii
A. Interview with Network Engineer on Secure WLAN Deployment xiv

ABSTRAK

Rangkaian network komputer telah menjejak ribuan langkah sejak kelahiran Wireless Local Area Network (WLAN). Faedah yang dicapai dari teknologi ini terdiri daripada kepuasan pekerja dan peningkatan productiviti secara keseluruhan setelah WLAN diimplikaskan. Namun, keselamatan masih lagi penting, biarpun kurang difahami dalam dunia teknologi maklumat. Pada tahun 2001, penyelidik melaporkan kelemahan dalam protokol IEEE 802.11b 'Wired Equivalent Privacy' (WEP). Cadangan langkah-langkah penyelesaian dari IEEE 802.11, IETF, Wi-Fi Alliance and OEMs dikaji untuk keselamatan dalam teknologi tanpa wayar. Suatu dasar WLAN yang menggunakan WEP dibina untuk mengawal keselamatan, dibina. Isu-isu sekuriti dalam WLAN yang dibentangkan oleh Network Computing pada 2002, digunakan untuk membentuk soalan-soalan temuduga dengan jurutera rangkaian untuk mengetahui isu keselamatan dan ancaman semasa implementasi WLAN. Tiga faktor utama menyumbang kepada suatu WLAN yang kuat. Teknologi merupakan faktor yang pertama. Integrasi antara WEP dengan Virtual Private Networking (VPN) dan IPSec, di sampingan 802.1X/EAP dan RADIUS pelayan, serta pangkalan data pengurusan yang berpusat dan polisi keselamatan, amat digalakkan untuk mengukuhkan sekuriti keseluruhan dan membolehkan capaian dihalang di pelbagai lapisan rangkaian. Di samping teknologi, manusia dan proses merupakan faktor-faktor bagi pengawalan keselamatan rangkaian di WLAN. Pekerja sepatutnya kerap menghadiri latihan dalam Polisi Keselamatan Teknologi Maklumat (IT), serta diberi kuasa untuk mengimplimentasikan Polisi Keselamatan IT, kerana ini tanggungjawab semua pekerja. Adalah menjadi mandat untuk membangunkan polisi keselamatan IT bagi mengawal semua dan teknik terbaik bagi meneruskan pengawalan keselamatan di syarikat setiap masa.

ABSTRACT (ENGLISH)

Computer network evolves with birth of Wireless Local Area Network (WLAN). Tangible benefits such as increase employee satisfaction and productivity drive enterprise WLANs adoption. However, security remains the most significant, but least understood in information technology. In the year 2001, academic researchers reported vulnerability in IEEE 802.11b Wired Equivalent Privacy (WEP) protocol. Solutions from IEEE 802.11, IETF, Wi-Fi Alliance and OEMs are studied for secure wireless solutions. A baseline WLAN which is solely secured by WEP is established. Concerns and security issues related to WLAN polled by Network Computing in 2002 is used to formulate the interview questions. Interviews with network engineers reviewed security issues and threats during enterprise WLAN deployment. Deploying and maintaining a secure WLAN is governed by three factors. The first factor is technology. Integration of WEP with Virtual Private Networking (VPN) and IPSec, plus 802.1X coupled with EAP and RADIUS server, on existing centralized administration database and security policy, are recommended to be handled layers to strengthen overall security and enable block access at multiple layers of the network. Besides technology, people and process also dictate security in WLAN. Employees should be trained constantly on IT Security Policy and empowered to enforce IT Security, as security is every employee's responsibility. It is a mandate to establish an IS Security Policy to regulate all process and best known methods to continuously maintain security of the enterprise.

CHAPTER ONE:INTRODUCTION

1.1. The Context of the Study

Wireless Local Area Networks (WLAN) are now in use in essentially every application amenable to implementation on a local area network. Five key application areas of WLANs, which provides networking functionality essentially identical to that on wire, but without the need to be tethered to the wall:

1. Vertical applications these continue to remain an important area of use for WLANs, typically involving data collection, bar codes, and industrial automation solutions. This is commonly exploited in warehouses and even in the cashier who diligently input the price of your purchase items in the shopping mall.
2. The enterprise the major growth area for WLANs over the past few years, microcellular-based WLANs allow roaming across a floor, building, campus, and even between facilities.
3. Small business smaller firms without dedicated network management and operations staff can benefit from the simplicity and ease-of-use inherent in wireless LANs.
4. The residence/home office homes are often much more difficult to wire than businesses, so wireless LANs in the home are rapidly growing in popularity and the mobility especially appeals to anyone who brings a notebook computer home from the office.
5. Public spaces one of the hot growth areas for WLANs over the next few years will be their deployment in "hot spots" within high-traffic public spaces airports, hotels, convention centers, and even coffee shops. In fact,

The contents of the thesis is for internal user only

Reference

1. LAN/MAN Standards Committee of the IEEE Computer Society. (1999). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band IEEE Standard 802.11, 1997 Edition.*
2. Goldberg, Ian., Rorisov, Nikita. & Wagner, David. (2001). *Intercepting Mobile Communications: The Insecurity of 802.11.* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
3. Arbaugh, William A., Shankar, Narendar., Wan, Y.C. Justin.. (2001). *Your 802.11 Wireless Network has No Clothes.* Department of Computer Science, University of Maryland, College Park, Maryland 20742 USA.
4. Lough, Daniel L., Blankenship, T. Keith. & Krizman. Kevin J. *A Short Tutorial on Wireless LANs and IEEE 802.11.* The Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia 24061-0111 USA.
5. Federal Information Processing Standards Publication 197. (November, 2001). *Announcing the Advanced Encryption Standard (AES).*
6. Posey, Brien M. (August, 2003). *WPA Wireless Security Offers Multiple Advantages Over WEP.* TechRepublic. http://techrepublic.com.com/5102-6265-5060773.html.
7. informIT. *Wireless Security.* http://www.informit.com
8. Fleck, Bob. & Dimov, Jordan. *Wireless Access Points and ARP Poisoning: Wireless Vulnerabilities That Expose the Wired Network.* Cigital Inc.. http://www.cigitallabs.com/resources/papers/download/arppoison.pdf.
9. AirDefense Inc.. (2002). 5 Practical Steps to Secure Your Wireless LAN.
10. Packet Cisco Systems Users Magazine. (First Quarter 2003). Securing Wireless.
11. Intel Corporation. (2000). *IEEE 802.11b High Rate Wireless Local Area Networks.* http://www.intel.com/ebusiness/wireless
12. Intel Corporation. (December 2002). *54 Mbps IEEE 802.11 Wireless LAN at 2.4 GHz.* http://www.intel.com/ebusiness/wireless.
13. Intel Corporation. (January 2003). *VPN and WEP: Wireless 802.11b Security in a Corporate Environment.* http://www.intel.com/ebusiness/wireless.
14. Intel Corporation. (February 2003). *Intel Building Blocks for Wireless LAN Security.* http://www.intel.com/ebusiness/wireless.
15. CIO Custom Publishing. (2003). *Securing Wireless Networks – Intel IT's Successful Journey.* http://www.intel.com/ebusiness/wireless

16. Microsoft Corporation. (1999). *Virtual Private Networking in Windows 2000: An Overview.*
17. Microsoft Corporation. (2002). *Mobility: Empowering People through Wireless Networks.* http://www.microsoft.com/technet/itsolutions/msit/security/secwlan.asp.
18. Microsoft Corporation. (2003). *Planning Guide 2 – Deciding on a Secure Wireless Networking Strategy.* http://www.microsoft.com/technet/security/prodtech/win2003/pkiwire/plan/swlanpg2.asp.
19. Microsoft Corporation. (2003). *Planning Guide 3 – Secure Wireless LAN Solution Architecture.* http://www.microsoft.com/technet/security/prodtech/win2003/pkiwire/plan/swlanpg3.asp.
20. Larry J. Blunk. & John R. Vollbrecht., (March 1998). RFC 2284. *PPP Extensible Authentication Protocol (EAP).* The Internet Society And The Internet Engineering Task Force.
21. Wi-Fi Alliance. (rev. 10/31/2002). *Overview Wi-Fi Protected Access.*
22. Wi-Fi Alliance. (rev. 2/6/2003). *Securing Wi-Fi Wireless Networks with Today's Technology.*
23. Wi-Fi Alliance. (rev. 2/6/2003). *Enterprise Solutions for Wireless LAN Security.*
24. Wi-Fi Alliance. (rev. 4/29/2003). *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*