SMARTAIR WIRELESS AUTHENTICATION SYSTEM

MOHAMED SHUKOR BIN OMAR

This report is submitted in partial fulfillment of the requirements for the
Bachelor of Computer Science
(Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2005

BORANG PENGESAHAN STATUS TESIS

JUDUL: SMARTAIR WIRELESS AUTHENTICATION SYSTEM

SESI PENGAJIAN: 2005

Saya MOHAMED SHUKOR BIN OMAR

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_____ TIDAK TERHAD

_____ _____

(TANDATANGAN PENULIS) (TANDATANGAN PENYELIA)

Alamat tetap : 1610 Kampong Kota,
13500, Permatang Pauh,
Butterworth.
Pulau Pinang.

Nazrulazhar Bahaman
(Nama Penyelia)

Tarikh : 24 NOVEMBER 2005 Tarikh : 24 NOVEMBER 2005

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.
^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

DECLARATION

I hereby declare that this project report entitled

SMARTAIR WIRELESS AUTHENTICATION SYSTEM

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date: 24 November 2005

(MOHAMED SHUKOR BIN OMAR)

SUPERVISOR: _____ Date: 24 November 2005

(MR. NAZRULAZHAR BAHAMAN)

DEDICATION

To my beloved mother and family, friends, my supervisor Mr. Nazrulazhar Bahaman and people who support me directly or indirectly……

ACKNOWLEDGEMENTS

Alhamdulillah. Syukur ke hadrat ilahi. Eventually my PSM report successfully completed. I would like to take this opportunity to thank my PSM supervisor, Mr. Nazrulazhar Bahaman for his kindly guidance and advices to complete this PSM report successfully.

I would also like to thank my beloved parents and family who have been giving me support and motivation throughout my project. My big thank also goes to my boss, Mr. Suhaimi Mohd and all friends for their help and support to complete my PSM report. Lastly, thank to the all people, who have giving support directly or indirectly. Thank a lot.

Warmest regards.

ABSTRACT

SmartAir Wireless Authentication is an internet wireless authentication for KUTKM community to use an internet service in KUTKM area. It provide safely and strictly authentication system with nice features. The main objective of SmartAir Wireless Authentication is to give an alternative way for KUTKM students and other campus community to having wireless internet service with concept *anytime & anywhere*. SmartAir Wireless Authentication could be a good solution for existing internet access facilities that have a limited internet access especially in student hostel and café or anywhere. The project brings a lot of advantages especially to college management to develop and manage the way of internet service with the authentication and made the service available in campus. The scopes of the project are enabling campus community to enter the authentication login before using the wireless internet service, deploy the installation and configuration of network services, drawing and illustrate the entire network. The significances of the project are for manage and authenticate the wireless internet network in order to more efficient and well-managed.

ABSTRAK

SmartAir Wireless Authentication ialah satu sistem penggunaan internet untuk warga KUTKM. Ia menyediakan sistem internet yang selamat dengan ciri-ciri yang baik. Objektif utama projek ini adalah untuk menyediakan jalan alternative untuk pelajar- pelajar KUTKM dan juga warga kampus yang lain untuk memperolehi perkhidmatan internet secara tanpa wayar dengan konsep *anytime & anywhere*. SmartAir Wireless Authentication dapat menjadi penyelesaian terhadap sistem internet sediada yang terhad seperti di asrama pelajar dan cafeteria. Projek yang bertajuk SmartAir Wireless Authentication System sememangnya membawa banyak kelebihan- kelebihan untuk digunakan terutama kepada pihak pengurusan KUTKM untuk mangurus dan membangunkan perkhidmatan internet tanpa wayar beserta keselamatan "authentication" di dalam kawasan kampus KUTKM. Skop projek ini pula adalah untuk membolehkan pengguna melalui paparan keselamatan sebelum menggunakan perkhidmatan internet tanpa wayar ini, juga membangunkan perkhidmatan rangkaian dan rekabentuk keseluruhan rangkaian. Akhir sekali, kepentingan projek ini adalah untuk mangurus pengguna dan keselamatan rangkaian internet tanpa wayar bagi manjadikannya lebih efisyen dan terkawal.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

802.11	-	IEEE Standard for wireless LAN
802.11b	-	First revision of 802.11 standard (11Mbps – 2.4GHz)
802.11g	-	An extension to 802.11b standard (54Mbps – 2.4Ghz)
802.11a	-	Second revision of 802.11 standard (54Mbps – 5Ghz)
802.1x	-	Security standard for WLAN
IEEE	-	Institute of Electrical and Electronic Engineer
LAN	-	Local Area Network
WLAN	-	Wireless Local Area Network
WAN	-	Wide Area Network
GHz	-	Gigahertz
Mbps	-	Megabits per second
ID	-	Identity
WEP	-	Wired Equivalent Privacy
MAC	-	Medium Access Control
RF	-	Radio Frequency
IP	-	Internet Protocol
DHCP	-	Dynamic Host Control Protocol
AP	-	Access Point
PEAP	-	Protected Extensible Authentication Protocol
CHAPv2	-	Challenge Handshake Authentication Protocol
TLS	-	Transport Layer Security
NMS	-	Network Management System
PDA	-	Personal Digital Assistant
OS	-	Operating System
PC	-	Personal Computer

SMTP	-	Simple Mail Transfer Protocol
SNMP	-	Simple Network Management Protocol
WiFi	-	Wide Fidelity
FAST	-	Framework for the Application of System Techniques
PCMCIA	-	Personal Computer Memory Card International Association
UTP	-	Unshielded Twisted Pairs
P&P	-	Plug & Play
USB	-	Universal Serial Base
BER	-	Bit Error Rate
DFD	-	Data Flow Diagram
ERD	-	Entity Relationship Diagram
FAQ	-	Frequently Asked Question
RADIUS	-	Remote Authentication Dial In User Services

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Project Background

The ***SmartAir*** represent a cross-section of campus areas that may benefit from wireless access. The different areas include library, lecture halls, café/ restaurant space, faculty areas and outdoor space. Other areas may include labs and conference rooms. The current wireless LAN standards are IEEE 802.11, operating in the 2.4GHz to 5.4GHz range and speed 11Mbps to 54Mbps. In KUTKM, the ideal areas to apply ***SmartAir*** include:

i. Library
ii. Faculties areas
iii. Cafeteria
iv. Lecture rooms

For the user subscription, especially for students, it is include in semester fee and every student will be provide the authentication account included username and password. The advance feature is ***SmartAir*** uses a web-based authentication scheme to authenticate a wireless session. Users open web and will redirected to the

SmartAir login page, where they need to enter their ***SmartAir*** ID and password. If authenticated, the user will be direct to their original web page and the popup window will come out for logout function.

1.2 Problem statements

The problem statement consist the authentication topic include new wireless authentication 802.1x and the supported protocols, platforms and wireless cards.

1.2.1 Authentication/ CHAP-Challenge and CHAP-Password

In the wireless LAN, accessing to wireless resources such as internet, file sharing and wireless peripherals same as wired LAN but authentication is very important topic. Authentication is the process of positive identification. Through many methods to perform authentication exist, the most common that computer users are familiar with is *password authentication*. Failure to understanding about authentication of system especially for Access Point and terminal may cause security attacks and resource such as internet connection easier for unauthorized people to use it. By default, ***SmartAir*** uses CHAP-Challenge and CHAP-Password. The advantage is that the web server and the "home" radius server will only know the actual passwords. Neither ***SmartAir*** nor any radius proxy servers get to know the actual password. CHAP-Challenge and CHAP-Password authentication is generally vulnerable to dictionary attacks.

There are some descriptions about Challenge Handshake Authentication Protocol for PPP or CHAP. Challenge Handshake Authentication Protocol (CHAP) used to verify the identity of the peer using a 3-way handshake. This done upon initial link establishment and may repeated any time after the link has been established. After the Link Establishment phase is complete, the authenticator sends a "challenge" message to the peer. The peer responds with a value calculated using a "one-way hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledge; otherwise the connection should be terminate. At random intervals, the authenticator sends a new challenge to the peer, and repeats steps 1 to 3.

CHAP provides protection against playback attack by the peer using an incrementally changing identifier and a variable challenge value. The use of repeated challenges intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges.

This authentication method depends upon a "secret" known only to the authenticator and that peer. The secret not sent over the link. Although the authentication is only one-way, by negotiating CHAP in both directions the same secret set may easily used for mutual authentication. Since CHAP may used to authenticate many different systems, name fields may used as an index to locate the proper secret in a large table of secrets. This also makes it possible to support more than one name/secret pair per system, and to change the secret in use at any time during the session. CHAP requires that the secret be available in plaintext form. Irreversibly encrypted password databases commonly available cannot used. It is not as useful for large installations, since every possible secret maintained at both ends of the link.

1.2.2 Supported protocols, platforms and wireless cards

There are many manufacturer involved in wireless industry like Cisco, 3Com, D-Link, SMC, Lucent, IP3 and much more. Many manufacturer means integration between them are small. Meanwhile, ***SmartAir*** is going to support PC, UNIX terminal under different OS such as Windows 2000 Pro and Linux Fedora or RedHat.

1.3 Objective

The main objectives of the ***SmartAir*** project are:

i. To provide new 'way' wireless internet connectivity and infrastructure to KUTKM network for used of students, staffs and guests. Most of the internet service area in KUTKM network wired access.

ii. Focus to the security and authentication of wireless internet connectivity. Web based authentication and wireless authentication must be seriously focus to keep away from any security attack or malicious usages.

iii. To makes the management system and internet facility more efficiency. The network admin can remotely control and monitor the ***SmartAir*** system from his place. Its will cut off the response time as well.

iv. To study the new wireless technology and apply it benefits to the campus environment. The staff can expose with new technology and interesting knowledge.

1.4 Scopes

The ***SmartAir*** Wireless LAN infrastructure is will implement physically as a design of network infrastructure. The main scopes are covered:

i. Deployment the wired and wireless infrastructure includes main server services, access point (AP), switch, router and LAN cabling. The wireless equipments like access point will connect to existing wired network. Wired network acts as bridge between wired and wireless network.

ii. Create web base authentication. There could be development of database application.

iii. Implement the system under different OS (Windows and UNIX), Linux Fedora Core 2 for server and Windows XP for mobile client.

1.5 Project significance

The ***SmartAir*** project absolutely bring a lot benefits to students, staffs and KUTKM management it self. For students, there is no more limitation of internet accessing in distance and wirelessly. They are able accessing an internet anywhere, anytime and any wireless platform whether their laptop, desktop and other wireless hand-held peripherals. ***SmartAir*** is ideal to implemented at these areas include library, faculty areas, Cafeteria and other suitable campus area. Most of KUTKM student owned a personal laptop. Students are able to accessing internet at anywhere their want as long within ***SmartAir*** coverage area without wires and they are authenticated user. KUTKM management also gets benefit of ***SmartAir*** because the charge of service is include in semester fee and every student must pay to provide the authentication account included username and password.

1.6 Conclusion

SmartAir wireless authentication system is the valuable project to develop in KUTKM environment and the wireless LAN technology can be the new way of communication. The wireless LAN standard brings a lot advantages for students, staffs, lectures and other campus community in network communication include wireless internet connectivity, freedom work anywhere, Quick, effortless installation, no cables to buy, Save cabling time and hassle and easy to expand. The SmartAir wireless authentication system also seriously focuses about security and authentication. The project scopes and the objective covered the entire requirement and the implementation need. Lastly, SmartAir wireless authentication system completes the network infrastructure for KUTKM.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

This chapter will describe the literature review for the currently project and the research that has been done. Literature review is being conduct to give an idea on how to solve the problem that being identified previously and to find out the solution for this project.

For the Project Methodology, *FAST* is the most excellent systems development process based on hypothetical methodology that used to demonstrate the project development process.

2.2 Fact and finding

For the fact and finding section, some searching, collecting, studying and analysing have been done for ***SmartAir*** project from the relevant sources include books, technical reference, web pages and case study:

2.2.1 Journals

A wireless campus environment provides user mobility, as user no longer tied to fixed locations to access the network. It also offers high network accessibility, as network resources remain accessible after office hours. While existing communication applications can work in a wireless network, they are separate applications that often require different device. This paper describes personal communication system that integrates various services into a unified platform, providing one-stop source for both information access and communication within a wireless campus environment. Using radio frequency technology, the wireless LAN transmit and receives data from one point to another over the air without relying on any physical wired connections. Thus, the wireless LAN supports user mobility and provides round-the-clock access to network resources. A wireless LAN system can be installed easily without the need to pull cable through walls and ceilings. [1] *Siu C. Hui, A. C. M. Fong, C. T. Lau. (2002). Campus Wide Information System, Volume 19, Number 1, pp. 27-35 (Emerald Journal).*

A look at computing literature in general and library literature in particular over the last few years reveals steadily increasing interest and investment by libraries in use of wireless Ethernet technology (802.11). This article attempts to shed light on the motivations underlying the use of this technology in a variety of libraries across the country as well as the role of the library in developing wireless within the local