MEASUREMENT AND COMPARISON BETWEEN WIRELESS NETWORK SECURITY (MAC ADDRESS FILTERING, EAP-TTLS AND PEAP-MSCHAPV2 (IPSEC))

MOHAMMAD YUSOF BIN ABU BAKAR

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS*

JUDUL: **MEASUREMENT AND COMPARISON BETWEEN WIRELESS NETWORK SECURITY (MAC ADDRESS FILTERING, EAP-TTLS AND PEAP-MSCHAPV2 (IPSEC))**

SESI PENGAJIAN: **2009/2010**

Saya **MOHAMMAD YUSOF BIN ABU BAKAR**
(HURUF BESAR)

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 Universiti Teknikal Malaysia Melaka
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)

Alamat tetap: No 2, Jln Kg Padang 5,
Kg Padang (Jln Sg Lembing)
25200 Kuantan
Pahang

Tarikh : 6/7/2011

(TANDATANGAN PENYELIA)

Dr Mohd Faizal Bin Abdollah
Nama Penyelia

Tarikh : 6/7/2011

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

MEASUREMENT AND COMPARISON BETWEEN WIRELESS NETWORK SECURITY (MAC ADDRESS FILTERING, EAP-TTLS, PEAP-MSCHAPv2 (IPsec))

MOHAMMAD YUSOF BIN ABU BAKAR

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2011

DECLARATION

I hereby declare this project report entitled

MEASUREMENT AND COMPARISON BETWEEN

WIRELESS NETWORK SECURITY
(MAC ADDRESS FILTERING, EAP-TTLS AND PEAP-MSCHAPV2 (IPSEC))

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

STUDENT : _____ Date: 6/7/2011

(MOHAMMAD YUSOF BIN ABU BAKAR)

SUPERVISOR : _____ Date: 6/7/2011

(DR MOHD FAIZAL BIN ABDOLLAH)

DEDICATION

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

To my supportive friends and my supervisor, thank you so much for assist and help.

ACKNOWLEDGEMENTS

First of all thanks to Allah because of his bless, I finally finished my PSM I successfully. I would to take this chance to express my gratitude to UTEM for provided chance enrolling this course and compulsory taken by all students. Many skills and experience I had obtained that never be taught in normal lecture and laboratory session by involving hand-on discipline in project management. These skills and experience only can be getting through practical experience by working on large project. All problems arise from this project and guide and maturing my decision and way of thinking. I'm very grateful to such person who always give supports and guide me to the right platform especially DR. MOHD FAIZAL BIN ABDOLLAH my supervisor. Without his concern, it is impossible to finish up this PSM project. Moreover, a big appreciation to my parents who are always giving me a morale supports and advices. Without their concern, it is impossible to finish up this project. Last but not least, thank you to my friends who give a lot of co-operation and suggest the solution for the problem. In the future, I already have an experience and confident to setup the network, especially wireless security for industrial training and the real job.

ABSTRACT

Wireless network refers to all types of computer networks that are not connected by any type of cable. The IEEE specifies the 802.11 standards are used for wireless LANs technologies. A wireless local area network (WLAN) links two or more devices use a wireless (radio) and typically provides wireless connectivity through an access point to the wider Internet. This gives users mobility to move within the local coverage area and still be connected to the network. Wireless technology also has advantages and disadvantages. The advantage of wireless is that implementation of low cost, flexible, ideal for places is not reasonable and so forth. The weakness of the wireless connection is lower speed compared to wired networks, complex configurations of cable networks and less secure. This project is specifically for wireless network security. This means, how to protect wireless networks from unauthorized users. There are many types of wireless authentication can be established. This project will use the Remote Authentication Dial In User Service (RADIUS) networking protocol. In addition, 802.1x authentications are also involved and it have concept of the three parties representing the supplicant, an authenticator and authentication server. There are three types of wireless authentication will be used for the project, which is the MAC address filtering, EAP-TTLS and PEAP-MSCHAPv2 (IPsec). The objective of the project is to study, compare and analyze the performance of the wireless authentication process. The results of these objectives will be used to select the most appropriate authentication method for wireless.

ABSTRAK

Rangkaian wayarles merujuk pada setiap jenis rangkaian komputer yang tidak disambung oleh mana-mana jenis kabel. IEEE menetapkan standard digunakan untuk teknologi LAN wayarles adalah 802.11. Sebuah kawasan rangkaian wayarles tempatan (WLAN) menghubungkan dua atau lebih peranti menggunakan sambungan (radio) wayarles dan biasanya menyediakan sambungan melalui pusat akses ke internet yang lebih luas. Hal ini memberikan pengguna mobiliti untuk bergerak dalam kawasan liputan tempatan dan masih boleh menyambung kepada rangkaian. Teknologi wayarles juga mempunyai kelebihan dan kekurangan. Kelebihan dari wayarles adalah kos perlaksanaan yang rendah,fleksibel, ideal untuk tempat-tempat tidak berpatutan dan sebagainya. Kelemahan sambungan wayarles ialah kelajuannya lebih rendah berbanding dengan rangkaian kabel, tatarajah kompleks dari rangkaian kabel dan kurang selamat. Projek ini lebih khusus untuk keselamatan rangkaian wayarles. Ini bererti, bagaimana untuk melindungi rangkaian wayarles dari pengguna yang tidak sah. Ada banyak jenis pengesahan wireless yang dapat dibentuk. Projek ini akan menggunakan Remote Authentication Dial Dalam User Service (RADIUS) protokol rangkaian. Selain itu, pengesahan 802.1x juga terlibat dan mempunyai konsep tiga parti yang merupakan pemohon, sebuah pegesahan dan pelayan pengesahan. Ada tiga jenis pengesahan wireless akan digunakan untuk projek, yang merupakan penapisan alamat MAC, EAP-TTLS dan PEAP-MSCHAPv2. Objektif projek adalah untuk mempelajari, membandingkan dan menganalisis prestasi setiap proses pengesahan wayarles. Hasil dari objektif tersebut akan digunakan untuk memilih kaedah pengesahan yang paling tepat untuk penggunaan wayarles.

TABLE OF CONTENTS

CHAPTER VI TESTING

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATONS

TERMS	DESCRIPTION
UTeM	Universiti Teknikal Malaysia Melaka
IEEE	Institute of Electrical and Electronics Engineers
Wi-Fi	Wireless Fidelity
LAN	Local Area Network
WLANs	Wireless Local Area Networks
ZOS	Zeroshell Operating System
RADIUS	Remote Authentication Dial-In User Service
PEAP	Protected Extensible Authentication Protocol
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol, version 2
EAP	Extensible Authentication Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
MAC address	Media Access Control address
IRC	Internet Relay Chat
URL	Uniform Resource Locator
NIC	Network Interface Card
IPsec	Internet Protocol Security
VPN	Virtual Private Network

CHAPTER I

INTRODUCTION

1.1 Project Background:

Computer networks can be built using either wired or wireless technology. Wired Ethernet has been the traditional, but Wi-Fi or wireless technologies are gaining ground fast. Both wired and wireless has advantages and disadvantages. Data is valuable information for an organization. Data can be transmitted in many ways, such as through a wired network (LAN) or wireless network (WLANs). A LAN physically links computers in an organization together via network cabling such as Ethernet CAT 5 cabling and run throughout wall and floors of organization building. A WLAN enables a local network of computers to exchange data or other information without use of cables. The data can be transmitted as radio signals through air. However, the security level for wireless networks is very weak and easily broken than wired networks.

This project is about wireless network security and IPSec network. Project implementation requires Zeroshell OS (ZOS) that acts as a RADIUS server and the authentication portal to access the internet. Zeroshell is a Linux distribution for servers and embedded devices aimed at providing the main network services a LAN requires. There are four mechanisms wireless networks that will be developed in this project which is MAC address filtering, EAP-TTLS and PEAP-MSCHAPv2 (IPsec).

After successful connected the network, client can browse the website provided in this project and use FTP service for transfer data between server and client. The Internet Relay Chat (IRC) server also provided in the network and client can use chat function to communicate and transfer file with other client. If client have the problem, they also can directly ask the question to the administrator using email. Every step to setup chatting client and email will be taught in the website pages.

1.2 Problem Statement

Wireless networking has great potential for improving access to services. For this reason, it has been rapidly increase for network connection. Unfortunately, many implementations are being done without attention to issues of security and authentication. As a result, most wireless networks with proper equipment can be access even from outside the building. Anyone with the proper equipment can also spy on traffic. They can see user's passwords as well as other data.

The problem statements in this project are:

- Every network interface card (NIC) has its own unique MAC address, and wireless access points can be configured to block all but a handful of specified NICs. The problem with MAC address, it easy to faked and readily detected by anyone using appropriate monitoring software.

- TTLS products are available from multiple vendors and have been proven interoperable by a number of public demonstrations. TTLS can be the run even though no integration certificated from client

1.3 Objective

i. To study authentication mechanism between MAC Address filtering, EAP-TTLS and PEAP-MSCHAPv2 (IPsec).

ii. To analyze the performance of each authentication mechanism.
- The performance will be measured from the authentication delay & response time between client and Access Point (AP)
- Measure the bandwidth and the quality of a network speed through FTP test.

iii. To compare level of security between wireless authentication in normal network and IPsec network.

iv. To select most appropriate authentication method for wireless.

1.4 Scope

i. This research will cover wireless authentication using RADIUS server and IPsec network.

ii. The research analysis related with wireless security and performance.

iii. The wireless network will be test in non-roaming situation.

1.5 Project significance

There are several benefit and significant of this proposed project. The result will be show the comparison between wireless authentications such as MAC addresses filtering, EAP-TTLS and PEAP-MSCHAPv2 (IPsec) in the wireless. Through the comparison, the research can be used as guide for wireless implementation. In addition, the network admin can use the research to improve wireless security in the future.

1.6 Expected output

In this project, the login credential will appear when user tries to connect access point. The users need to enter username, password and domain for pass the RADIUS credential. After that, the captive portal will appear and ask the users to enter username and password to get access the internet connection. The implementation of IPsec network need certificated at both client and server side to communicate each other. After successful connected the network, user can chat and send email with other client in the network. They also can communicate and share file with other users in chat room. The analysis result will be used as guide for choosing the best wireless security.

1.7 Conclusion

This chapter gives explanation about the project background, problem statement, objective, scope and project significant and also expected output of the project. This PSM project is to study the level of wireless security and analyze the wireless performance. The best wireless authentication will be choose between MAC Address filtering, EAP-TTLS and PEAP-MSCHAPv2 (IPsec). This project also helps students to improve skills and provide experience for individual projects. In addition, this project is one way to save costs because it does not require expensive devices to develop. In the coming of the second chapter of this project is about the literature review and project methodology, it will be focused on the findings and the methodology of the projects.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

This chapter, explain about the software and hardware which are going to be in the research. This chapter also discuss about comparison between the previous researches. A literature review is to review the important points of current knowledge. Literature reviews are secondary sources, and do not report any new or original work.

Project methodology is an important part to design and develop project especially in wireless network project. It will show what the methodology and method use in network design to build up the project. Before choose what the methodology for the project, developer is consider made a research related with the project. This topic also briefly explain about the project requirement includes hardware, software and network, project schedule and milestone and conclusion.