SECURE WIRELESS COMMUNICATION BETWEEN PC AND ANDROID MOBILE DEVICE

MUHAMAD HAFEZE BIN MUHAMAD HASANI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LAMPIRAN B: BORANG PENGESAHAN STATUS TESIS

BORANG PENGESAHAN STATUS TESIS*

JUDUL: SECURE WIRELESS COMMUNICATION BETWEEN PC AND ANDROID MOBILE DEVICE

SESI PENGAJIAN:

Saya MUHAMAD HAFEZE BIN MUHAMAD HASANI, mengaku membenarkan tesis (PSM) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek 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)	(TANDATANGAN PENYELIA)
Alamat tetap: Lot 2819, Bt 2 ½ Jln Belimbing, Meru, 42200 Klang, Selangor Darul Ehsan.	DR.MOHD FAIZAL ABDOLLAH Nama Penyelia
Tarikh:_____.	Tarikh:_____.

CATATAN:

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

SECURE WIRELESS COMMUNICATION BETWEEN PC AND ANDROID MOBILE DEVICE

MUHAMAD HAFEZE BIN MUHAMAD HASANI

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2014

DECLARATION

I hereby declare that this project report entitled

SECURE WIRELESS COMMUNICATION BETWEEN PC AND ANDROID MOBILE DEVICE

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

STUDENT: _____ Date: _____.
(MUHAMAD HAFEZE BIN MUHAMAD HASANI)

SUPERVISOR: _____ Date: _____.
(DR.MOHD FAIZAL ABDOLLAH)

DEDICATION

Alhamdulillah, praise to Allah…

Tuan Haji Muhamad Hasani Bin Ahmad and Puan Haji Norzita Binti Taip,
I'm glad to be your son and I'm very thankful to Allah to have father and mother like you. Thanks for giving me support to further my study...
I hope that I'm able to payback all sacrifice that you have made...

Awie, Faiz, Wawa and all my friends that together in completing this fyp also was giving me help and support, thank you guys...

Prof. Madya Dr. Mohd Faizal Bin Abdollah,
Many thanks for your guidance, advice and consideration that you have been given to me in completing this fyp...

To UTeM librarians, thank you for helping me in process of borrowing books. To UTeM guards and FTMK staff such as lecturers, staff offices, and cleaner, thanks a lot for the help and provides a comfortable place for me to do my fyp...

THANK YOU!

ACKNOWLEDGEMENTS

In the name of Allah, the most gracious and the most merciful…

Alhamdulillah, all praises to Allah for the strengths and blessings in completing this fyp. I would like to thank my beloved parents who have been giving me support and motivation throughout my fyp. I also would like to thank Dr. Mohd Faizal Abdollah for giving assistant to complete this fyp successfully. Not forgotten, I would like to thank all my lecturers for providing me a lot of knowledge and never give up teaching students for better future. Last but not least, I would like to thank my housemates, classmates, labmates and other friends who have support, helps and encourage me during the completion of this fyp.

ABSTRACT

There are many threats when sending data packets through the network traffic, particularly the public traffic network (internet). Even so, there are security mechanisms that can be used to secure connections such as IPSec to ensure data integrity. This project is the simulation of secure communication between the server and Android mobile devices. By using Openswan IPSec VPN tunnels and authentication by FreeRADIUS, a packet will be encrypted and secure from any unauthorized third parties using techniques eavesdrop.

ABSTRACT

Terdapat banyak ancaman semasa menghantar paket data melalui rangkaian trafik terutama rangkaian trafik awam (internet). Walaupun begitu, terdapat mekanisma keselamatan yang boleh digunakan untuk menjamin sambungan seperti IPSec untuk memastikan integriti data. Projek ini adalah mengenai simulasi komunikasi yang selamat di antara server dan peranti mudah alih Android. Dengan menggunakan terowong Openswan IPSec VPN dan pengesahan oleh FreeRADIUS, paket akan disulitkan dan selamat daripada mana-mana pihak ketiga tanpa kebenaran yang menggunakan teknik eavesdrop.

TABLE OF CONTENTS

CHAPTER 2 LITERATURE REVIEWS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATONS

PC	Personal Computer
IP	Internet Protocol
AAA	Authentication, Authorization, and Accounting
AH	Authentication Header
AP	Access Point
API	Application Programming Interface
CA	Certificate Authority
CHAP	Challenge-Handshake Authentication Protocol
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKE	Internet Key Exchange
IMEI	International Mobile Station Equipment Identity
IMS	Internet Protocol Multimedia Subsystem
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ITU-T	ITU Telecommunication Standardization Sector
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control

MSCHAP	Microsoft Challenge-Handshake Authentication Protocol
NAT	Network Address Translation
OHA	Open Handset Alliance
OS	Operating System
PAP	Password Authentication Protocol
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PPP	Point-to-Point
PPTP	Point-to-Point Tunnelling Protocol
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial in User Service
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
SA	Security Association
SDLC	System Development Life Cycle
SPI	Security Parameter Index
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VM	Virtual Machine
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XL2TPD	Xelerance Layer 2 Tunneling Protocol Daemon

CHAPTER 1

INTRODUCTION

1.1 Introduction

Communication between two various devices via wireless connection has been used widely. There are many advantages and disadvantages of using this technology. Lack of security of the packet data that travels through this medium are one of the disadvantages of it. Even so, there are many security mechanisms can be used to secure the connections. Android by Google are one of the OS that use wireless as their medium of communication to communicate with another wireless devices.

Hence, in this project, a connection between a host (PC) that will act as a main server and Android mobile device that will act as a client will be established. In order to secure the connection between this two devices, security mechanism will be applied to ensure the confidentiality, integrity, and availability of the data. Therefore, this project will demonstrate a secure wireless communication between PC and Android mobile device.

1.2 Project Background

IP packets doesn't have any security features, making each of it transmitted through network medium are easy to sniffed by eavesdropping technique. Hence, there is no guarantee that each of it is from the claimed sender, was not sniffed during transit, or contains the original data without being changed. IPSec is a security mechanism that provides a protection to IP datagram by defining a method for specifying the traffic to protect, how the traffic will be protected, and also to whom the traffic is being sent. IPSec covers IPv4 and IPv6 with offering two types of protocols; AH and ESP [Craig Shue et al, 2005].

RADIUS is a popular security protocol that act as a gatekeeper for ISPs. Even so, it is capable of so much more than that. There are a lot of types of RADIUS servers as well as a lot of ways to configuring it [Brien Posey, 2006]. With the increasing of remote users try to access the network, RADIUS is widely used to control it. It manages and secures the WLAN, remote VPN, and wired access. Users are authenticated by the RADIUS server against a central database [Daniel Szilagyi et al, 2009].

Android OS developed by Google Inc. has become a very popular as one of the OS for mobile devices such as smartphones and tablets. Some of the features is it provides a short transport technology via wireless but in the same time, many threats linked with this platform such as malware also increasing. There is a study on security matters with Android devices. In that study, an implementation of a security channel of communication with VPN had been done [Angel Alonso-Parrizas, 2011]. In the case of users connected to other Android using Wi-Fi need to be discuss how to ensure the security of communication between the host and client.

There is several free apps in the internet can be used for establishing virtual private network such as Openswan, OpenVPN, SocialVPN and some more. Each of software provides different method and protocol. This project will establish an IPSec VPN in IPv4 network via using the open-source software: Openswan IPSec and will be authenticated by FreeRADIUS.

1.3 Problem Statement

An important thing in sharing files is the security of the file to be shared. There are many hackers out there who will take advantage of the file that is in the process of file sharing to exploit for personal gain. The Problem Statement (PS) is summarized into Table 1.1:

Table 1.1: Summary of Problem Statement

No	Problem Statement
PS1	There is a lack of relevant safety issues in sharing files using wireless connection between two devices; PC to Android mobile device for example.

1.4 Project Questions

The security matters in exchanging of data through wireless connection between PC and Android device cannot be guaranteed. So that, it needed to be figured out what is the definition of secure wireless communication. In which way to secure the connection and how to implement the solution need to be done. The summarizations of the Project Questions (PQ) are shown in the Table 1.2:

Table 1.2: Summary of Project Question

PS	PQ	Project Questions
PS1	PQ1	What is a secure wireless communication between PC and Android mobile device?
	PQ2	How a secure wireless communication between PC and Android mobile device can be established?
	PQ3	How the secured wireless communications between PC and Android can be proven?

1.5 Project Objectives

Based on the project questions formulated in previous section, appropriate Project Objectives (PO) is developed as in Table 1.3:

Table 1.3: Summary of Project Objectives

PS	PQ	PO	Project Objectives
PS1	PQ1	PO1	To study how to secure wireless communication between PC and Android mobile device.
	PQ2	PO2	To establish a secure wireless communication that allows PC and Android mobile device sharing data without being tracked or sniffed.
	PQ3	PO3	To test and validate a secure wireless communication that has been established

1.6 Project Contribution

Since security matters in exchanging data between PC and Android device became an issue, developing a secure wireless communication will help the community to address the problem thus provides a medium for them to exchange data securely.

1.7 Project Scope

The project will be focused on:

- Linux Ubuntu OS 12.04.3
- Android OS (2.3.6 GingerBread)
- Openswan IPSec VPN
- L2tp (XL2TPD)
- FreeRADIUS

1.8 Project Significant

This secure wireless communication will hopefully help user especially Android phone user to share their data such as documents, pictures and other data with other connected PC user through wireless connection in secure line.

1.9 Project Output

At the end of this project, a secured wireless communication between PC and Android mobile device will be demonstrated and using Wireshark application, the packet data will be analysed to confirm it is securely transferred.

1.10 Report Organization

This report consist of six chapter namely Chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Design and Implementation, Chapter 5: Testing and Result Analysis and Chapter 6: Conclusion.

Chapter 1: Introduction

This chapter will discuss about introduction, project background, research problem, research objective, scope, project significant and report organization.

Chapter 2: Literature Review

This chapter will explain related work of this project of android application language and tools.

Chapter 3: Methodology

This chapter will explain the method used and organise the sequence of project work in phase by phase.

Chapter 4: Design and Implementation

This chapter will introduce the software and hardware use in this project, environment setup, implementation of android application as well as the data collected.

Chapter 5: Testing and Result Analysis

This chapter will analyse the collected data and carry out the scripting proposed to support the evidence.

Chapter 6: Conclusion

This chapter will concludes and discussed the finding, limitations, contribution and the future work of the project.

1.11 Conclusion

Wireless communication is widely used nowadays. In line with the increase, many security threats exist. Thus, a secure wireless connection need to be implemented to assure the originality, confidentiality and availability for each packet of data that being transmitted is safe.

IPSec is one of the protocol suites that able to secure IP communications by authenticating and encrypting each IP packet of a communication session. The VPN servers are a gateway that control access to the network and has a RADIUS client component that communicates with the RADIUS server [cisco.com, 2006]. With implementing an IPSec VPN using open-source software Openswan and an authentication by RADIUS, a secure wireless communication can be established.