GUAY WEI LIN MASTER OF. ENG. (COMPUTER & MICROELECTRONIC SYSTEM) 2007 UTM

SECURE OPEN WIRELESS LAN USING POINT TO POINT PROTOCOL

GUAY WEI LIN

UNIVERSITI TEKNOLOGI MALAYSIA

To my beloved mother, father and sisters

ACKNOWLEDGEMENT

First of all, I wish to express my sincere appreciation to my supervisor, Professor Dr. Norsheila binti Fisal, for her encouragement, and guidance.

Besides, I would like thanks to Intel Microelectronics (M) Sdn. Bhd for funding my part-time Master study. My manager, Intel-University staffs, UTM School of Postgraduate Study and Faculty of Electrical Engineering staffs also deserve special thanks for their assistance in providing stable and comfortable environment for me to focus on my research.

Lastly, I would like to thanks all the lecturers, course mates and friends that have helped me through during the period on completing this research.

ABSTRACT

There are several approaches to achieve secure WLAN access network. One class of solution which will be commonly used is based on enhanced security within the IEEE 802.11 and WI-FI. Protected Access (WPA). In another class solution, the mobile station uses Point-to-Point Protocol (PPP) to establish a point-to-point tunnel to some devices normally located in the access network. Since PPP provides access control features independent of network or higher layer protocol and since it is a mature protocol with support on all major platform, it is also a good candidate for implementing a NAS in shared WLAN environment. To establish the PPP tunnel in a LAN environment, techniques such as low level PPP over the Ethernet protocol (PPPoE), or the higher level Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) can be used. This research will be focus on adding an additional layer on top of WLAN MAC using PPP to increase the security. The work will be carried out on WLAN testbed connected to the Internet.

.

ABSTRAK

Kaedah pencegahan pencerobohan capaian wireless LAN boleh dikategorikan kepada beberapa kategori. Satu kaedah umum yang biasa digunakan ialah menggunkan IEEE 802.11 atau dinamakan sebagai WPA. Selain daripada itu, cara yang lebih efisyen ialah mengehadkan klien-klien yang ingin mendapat internet perlu meggunakan PPP (point-to-point Protocol) untuk menjalinkan satu hubungan sebelum boleh dicapai. Dengan penggunaan kaedah ini yang mengguna semula satu lagi protokol yang matang antara layer antasan dengan layer bawahan juga boleh diimplementaikan until NAS. Dalam projek ini, penyelidikan akan dijalankan until menambahkan satu layer tambahan atas MAC dengan PPP untuk mengekuatkan keselamatan WLAN.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

CHAP	–	Challenge Handshake Authentication Protocol
GUI	–	Graphical User Interface
IOCTL	–	Input/Output Control (System Call)
MAC	–	Medium Access Control
OSI	–	Open System Interconnect
PPP	–	Point to Point Protocol
PPPOE	–	Point to Point over Ethernet
RAD	–	Rapid Application Development
WEP	–	Wired Equivalent Privacy

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

WLAN is a wireless local area network, which link two or more computers without using wires. It uses radio frequencies to accomplish the same functionality that a wired LAN has. Today, the number of organizations that are deploying the wireless networks increases tremendously where mostly utilizing the IEEE 802.11x protocol. Even though wireless LAN provides the luxurious of mobility to the end user, it has the disadvantages compare with LAN especially the security matter. Due to the fact that wireless LAN share transmission medium, it is more vulnerable compare with wired LAN which has a dedicated PHY connection.

Although attempts have been made to secure these networks; the technology used is intrinsically insecure and still highly susceptible to active attacks and passive intrusions. Standard tools for monitoring wired networks and ensuring their security examine only network (layer 3) or higher abstraction layers based on the assumption that the lower layers are protected by the physical security of the wires. However, this assumption cannot be extrapolated to wireless networks because of the broadcast

nature of such networks. Ideally, an intrusion detection system for wireless networks should function at the data link layer (layer 2) or even lower if extremely high security is required.

Thus, in this research, an additional layer will be introduced on top of the 802.11x MAC layer with PPP to increase the security of WLAN.

1.2 Problem statement

Wireless LAN is one of the emerging technologies; however, wireless LAN is more insecure than the wired LAN. There are seven major risks of wireless LAN attack which discuss below.

First of all, the most common attack is named as insertion attacks which means the attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review. For instance, unauthorized clients or unauthorized access points.

Secondly, interception and unauthorized of wireless traffic is also one of the popular network hacking cases. The interception happened when the network intruder intercept the wireless traffic within the range of an access point. Once the intruder manages to access the network data stream, several methods can be used to hack into the wireless LAN such as AP clone traffic interception, wireless packet analysis and broadcast monitoring.

Thirdly, jamming which is the denial of service attacks. This attack also easily applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency,

corrupting the signal until the wireless network ceases to function. In addition, cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

Fourthly, client-to-Client attack occurred when two wireless clients can talk directly to each other, bypassing the access point. In this case, all the communication is out of the access point control.

Fifthly, Brute force attacks against access point passwords. As today, most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing every possible password.

Sixthly, the encryption attack against the WEP of the access point is also the root causes for the insecurity of wireless LAN. 802.11b standard uses an encryption system called WEP (Wired Equivalent Privacy) while it has known weaknesses especially on the effective key size only valid for 40 and 104 bit even commercial claimed key size are 64 and 128 bit. The lesser the key open the gate for the hackers to crack the key easily.

Lastly, default configuration on the access point, many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment.. For example, the default SSID for linksys AP will is “Linksys”. Both these

The above seven attacks are the major risks of today wireless LAN network where some of the attacks can be avoided by implementing different type of intrusion detection approaches. In this research, one of the approach has been carried out which is using the PPP on the data link layer to enhance the authentication method.

1.3 Goals

The major goals of this research will be implement a PPP data link layer over the wireless LAN MAC layer with the purpose to reduce the vulnerability of existing IEEE 802.11b network.

1.4 Objectives

The project is carried out based on the following objectives. Below will be the three main objectives of this project.

Firstly, implement wireless intrusion detection system that builds on the data link layer. In this case, PPP is the data link layer that has been selected to be added.

Secondly, the purpose of adding the intrusion detection system at the data link layer is to improve the security of 802.11b wireless network.

Thirdly, reuse the mature protocol, PPP (point-to-point protocol) connection to integrate with the existing 802.11b to enhance the authentication layer as a way to avoid the active attack.

1.5 Scope

Based on the availability of the hardware and software, this research has been narrowed down with the following scopes:

- The API of this project will develop an additional PPP layer on top of the existing 802.11b MAC layer regardless using open authentication or WEP.
- The application will be written using C/C++ programming language for the core API while the GUI is developed using the Java OO programming language.
- The application is based on Intel 2200ABG wireless NIC card drivers, which is the source forge open source device driver. Other wireless NIC card can be used as long as the device drivers for LINUX can be obtained.
- The application is targeted on Linux environment (Fedora Core 6.0) as the Fedora core is the development environment.
- The application of this research will not improve the performance of RF signaling/coexistence between RF devices.
- This application will not support multilink PPP but it is recommended to support multilink PPP as a future work.
- This project will not judge the throughput comparison between PPPoE and PPP over wireless LAN.
- Assumption has been made that 802.11b PHY is working fine and noise-free where changes are only limited on the Data Link layer as the lowest layer.

1.6 Project Outline

This report of this project will be divided into 6 main chapters. The first chapter will discuss the objectives, scope and goals of this project. It discusses the first stage of the RAD (rapid application development) phase which will be requirement planning stage. In this stage, the main focus will be on defining the right objectives, scope and goals.

In the chapter 2, it covers the literature review where the study on the existing specifications and paper such as the RFC PPPOE, RFC CHAP that has been published on the RFC website. Besides, a thorough discussion on the wireless LAN has been carried out to provide a details understanding of the main topics, wireless LAN.

In chapter 3, the report covers the software methodology that has been picked to develop the application of this project. RAD (Rapid application development) has been chosen for this project.

In chapter 4, which will be the System Analysis and Design where discusses on how to design the whole application from the system architecture perspective as well as the software architecture viewpoint.

In chapter 5, the implementation and result chapter covers the details explanation of the code that written for the API as well as the GUI. At the second part of the chapter, the reports illustrate the output trace that has been captured based on the application that has been developed.

In the last chapter, chapter 6 which will be the summary and conclusion chapter summarized the entire project and ended with the potential future works that can be carried out.