HYBRID SECURITY MECHANISM IN WIRELESS LOCAL AREA NETWORKS (WLANS)

BY
EILEEN JOSEPHINE G. CLEMENCIO
LEAH LYNN F. DACUA
BRYAN ECHART S. QUIÑONES

SCHOOL OF ARTS AND SCIENCES
ATENEO DE DAVAO UNIVERSITY

MARCH 2006

HYBRID SECURITY MECHANISM IN WIRELESS LOCAL AREA NETWORKS (WLANS)

AN INDEPENDENT RESEARCH
PRESENTED TO
THE FACULTY OF THE COMPUTER STUDIES DIVISION
ATENEO DE DAVAO UNIVERSITY

IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE
BACHELOR OF SCIENCE MAJOR IN COMPUTER SCIENCE

BY
EILEEN JOSEPHINE G. CLEMENCIO
LEAH LYNN F. DACUA
BRYAN ECHART S. QUIÑONES

SCHOOL OF ARTS AND SCIENCES
ATENEO DE DAVAO UNIVERSITY

MARCH 2006

TABLE OF CONTENTS

Thesis Summary

Hybrid Security Mechanism in Wireless Local Area Networks (WLANs)

by

Clemencio, Eileen Josephine G.
Dacua, Leah Lynn F.
Quiñones, Bryan Echart S.

Abstract:

A Wireless local area network or WLAN has two major components to its security problem. These are the privacy of the transmitted data and the protection against intrusion. There are several security problems of Wi-Fi. Examples of these are: easy access, rogue or unauthorized wireless devices, unauthorized use of service, service and performance constraints, MAC spoofing and session hijacking, traffic analysis and eavesdropping, and higher level attacks. There have been measures that have been made to address these problems, and this led to the creation of many technologies that offer to provide security means to unsecured networks such as wireless LANs or Wi-Fi. However, these technologies are often limited to one security problem. Those that provide overall network security only provide an adequate amount of security. This thesis will create a hybrid security mechanism based from existing security mechanisms that can answer to the security problems of Wi-Fi, especially the problem on unauthorized access.

Keywords:
Wi-Fi, spoofing, eavesdropping

Chapter I

INTRODUCTION

1.1 Background of the Study

In our modern world, people often go for the new technologies available in the market to make their work easier. One of these technologies is wireless LAN or Wireless Fidelity (Wi-Fi).

The primary reason for building a wireless local area network (WLAN) is for improved mobility. One can move around from room to room without being tethered to a network jack. Another reason people like wireless LANs is because they can network their computers together without having to snake wires through their walls.

If one thinks about building a wireless network for their home or office, it pays to do a little planning to ensure that they implement it as securely as possible. Security has long been a problem of the wireless industry. One of these is rogue or unauthorized wireless devices that can be used to attack the network or other networks, or have unauthorized access. These devices can be means to steal bandwidth, retrieve confidential data, attack a network, or use a network to attack other networks.

Currently, the information technology industry is still addressing the problem of wireless LANs with new solutions for manageable and acceptable network security. Because of this, there is a need to study this area and contribute a solution to this security threat.

1.2 Statement of the Problem

This study seeks to answer the following general problem: How can we enhance the security of a wireless local area network (WLAN) to minimize the threat of unauthorized access?

Specifically, it seeks to answer the following questions:

- What are the existing security mechanisms that are present today?
- What are the characteristics of the wireless device (wireless router) which will be used in the study?
- In addition, what are the security mechanisms supported by its firmware?
- What protocols would be allowed on the wireless network?
- How can the team immediately block an unauthorized access?
- In what area can the team enhance the security of a wireless network?

1.3 Objectives of the Study

The general objective of this study is to enhance security of a wireless Local Area Network (WLAN) to minimize the threat of unauthorized access.

The specific objectives are:

- To identify the existing security mechanisms those that are present today.
- To determine the characteristics of the wireless device (wireless router) which will be used in this study.
- To determine the security mechanisms supported by its firmware.
- To identify the protocols that would be allowed on the wireless network.
- To know how we can immediately block an unauthorized access.

- To know the area were the team can implement this new security mechanism in a Wireless network.

1.4 Scope and Limitation of the Study

This study generally focused on the existing security mechanisms of WLANs in dealing with unauthorized access. A hybrid security mechanism is developed, which is basically a consolidation of a number of the best security mechanisms on the market that can further prevent the threats of unauthorized access in a wireless network. The new hybrid security mechanism covers authentication, confidentiality, access control, and integrity issues in wireless networks. Since the router obtained has a firmware that supports MAC Filtering, Allotting of IPs, WPA and Closed System, the study is focused on Protocol Filtering and the Intrusion Detection System. Since the open sourced firmware that is enhanced is developed in the Linux Operating System, it can only be used on wireless routers with the same Operating System (Linksys versions 4 and below). Furthermore, it is aimed at defeating easy and unauthorized access to a wireless network, service and performance constraints, more specifically the denial of service, spoofing and unauthorized access, session hijacking and modifying, and sniffing and eavesdropping. This study is focused on wireless local area networks at home or in small businesses only. This does not include large companies for they require more intensive research and have more complex security needs.

1.5 Significance of the Study

Many internal Wi-Fi security problems occur when users purposely or accidentally deactivate traditional firewall and antivirus software installed on their computers. Additional problems arise when uninformed users deploy new wireless devices on their own in small businesses with a wireless network or when people establish their own wireless networks at their homes. Since clients or wireless hosts of a wireless network automatically choose the best available Wireless Router or Wireless Access Point nearby and connects with it, wireless clients from one network can connect to Wireless Routers or Wireless Access Points from a neighboring network if they are in the same area.

Having been presented with the potential threats of unauthorized connections, whether intentional or unintentional, such connections can bring a big hole in a network security which exposes critical data to outsiders. Moreover, networks with inferior security measures are prone to outsiders who are out to steal bandwidth, retrieve confidential data, attack business assets, or use the network to attack others.

This study can provide home and small business wireless networks with better defense against unauthorized access by the hybrid security mechanism that addresses the threats mentioned. Since the firmware, where the hybrid security mechanism is placed, is compatible with Linksys Wireless Routers versions 4 and below, people can enjoy their old Wireless Router with stronger security. People with old Wireless Router don't have to buy new ones just to have better security, but rather use the enhanced firmware from this study.

1.6 Definition of Terms

Asymmetric keys

Asymmetric algorithms use pairs of keys. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called "private key" or "secret key", while the encryption key is spread to all who might want to send encrypted messages, therefore called "public key". Everybody having the public key is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key.

Checksum

This is a simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled.

Ciphertext

Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.

Closed system

This is a technique developed by Lucent wherein access points do not broadcast SSID beacon frames.

Crack

This is copying commercial software illegally by breaking (cracking) the various copy-protection and registration techniques being used.

Data encryption

This is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, there must be access to a secret key or password that enables the user to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

Eavesdropping

These are attacks that involve any form of subversive *interception* of information can be categorized as either "eavesdropping" or "sniffing." The term "sniffing" usually refers specifically to non-intrusive and often undetectable interception, such as by reading information that is broadcast or by attaching a passive listener to a communication channel. The term "eavesdropping" is a less technical term and applies more broadly and loosely.

This category of attacks often involves the use of a "covert channel." A *covert channel* is any communication pathway that exists but was not intended by the designers of the system and thereby violates the system's security policy. A covert channel need not be an actual mechanism intended for *any* form of communication at all; for example, the technique of varying the load on a CPU

has been used as a covert channel for the binary encoded signaling of sensitive information to another process in an undetected manner.

Firewall

This is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firmware

Firmware consists of software programs and data that define the device's configuration and are installed semi-permanently into memory using various types of programmable ROM chips, such as PROMS, EPROMs, EEPROMs, and flash chips.

Frames

This is the unit of data transferred across the network, defined at the datalink (network access) layer of the protocol stack.

Intrusion Detection System (IDS)

There are two main types of intrusion detection systems: host-based and network-based. The former is generally founded on the idea of monitoring a system for changes to its file system and the latter on the other hand inspects network traffic.

MAC filtering

This is creating a secure Wi-Fi network by using the MAC address of each Wi-Fi device on the network (and only allowing devices with a known MAC address).

Packets

This is the unit of data at any layer of the protocol stack, prior to, or after transmission.

Protocol

This is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection.

Repository

A repository is a central place where data is stored and maintained. A repository can be a place where multiple databases or files are located for distribution over a network, or a repository can be a location that is directly accessible to the user without having to travel across a network.

Snippet

This is a small piece of program code.

Snooping

This is an unauthorized access to another person's or company's data. The practice is similar to eavesdropping, but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Spoofing

Spoofing involves forging or corrupting (destroying the integrity of) a resource or artifact for the purpose of pretending to be—i.e., for the purpose of masquerading as—something or someone else.

Static IP address

This is an IP address that does not change.

Wi-Fi

Short for wireless fidelity, is the Wi-Fi Alliance's name for a wireless standard, or protocol, used for wireless networking using the 802.11 standards.

Wireless Access point

This is a broadcast station that Wi-Fi computers can communicate with. It is also called AP, hotspot, and base station. Access points are used as the central point for a network of Wi-Fi computers.

Wireless Router

This is a hardware device or a software program that allows one network to connect to another. In a home network a wireless router can be used to

connect a wireless LAN to the large network of interconnecting networks called the Internet. An access point with a built-in router can be bought. The router will allow one to share a single Internet connection among all the computers connected to the network.