802.11 Person-In-Middle (PiM) Attacks:

Implementation and Practical Solutions

A Thesis
in TCC 402

Presented to

The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science in Computer Science

by

Chang Yuan-Yao (Jeffrey)

3/23/2004

On my honor as a University student, on this assignment I have neither given nor received unauthorized aid as defined by the Honor Guidelines for Papers in TCC courses.

Signed_____

Approved _____ Date _____
Technical Advisor – David Evans

Approved _____ Date _____
TCC Advisor – Helen Benet-Goodman

Table of Contents

Table of Figures

Abstract

The IEEE 802.11 is one of the very first wireless local area network standards that is currently widely deployed. Much research has been done on the IEEE 802.11 wireless network standard and the standard is known for its insecurity. Several reports have addressed the 802.11-based network vulnerabilities mainly for its lack of authentication. This thesis project depicts a specific Internet attack called the Person-in-Middle attack. The Person-in-Middle attack is a threatening attack that in the worst situation could fully control any computer in the wireless network. By designing and recommending four solutions to the attack, the thesis project will hopefully enhance the current IEEE 802.11 security.

This thesis project also aims to improve the IEEE 802.11 standard by analyzing the security mechanisms the standard provides. The IEEE 802.11 standard provides basic security mechanisms such as the wired equivalent protocol, an encryption protocol, and the media access based access control list, which is essentially a list of legitimate clients. Attackers may easily penetrate these IEEE 802.11 basic security mechanisms.

Out of the four solutions proposed in this thesis document, the Third Party PiM Attack Detector is optimal in terms of cost and the time it takes to deploy the solution. Due to time constraints and ethical reasons, I did not perform any testing of the PiM attack solutions. Successors of this thesis project should implement the PiM attack and test out all four solutions.

Chapter One: Introduction to Thesis Project

The Internet boom during the 20th century created much commercial opportunities for organizations. From the early Internet access technologies of modem dial-ups to Digital Subscriber Lines or cable modems, the fast improvement of the Internet has never ceased. As the speed of Internet access increases, people began to focus on improving the mobility and portability of computers accessing the Internet. Most organizations now deploy wireless local area networks (WLAN) as a convenient way of providing Internet access [1]. WLANs differ from the normal local area networks mainly in WLAN's ability to use radio signals as opposed to physical wires to transmit data. A major problem with transmitting data as radio frequencies resides in the fact that they are easy to intercept. Any computer with WLAN accessible hardware is capable of intercepting data transmitted by another computer in the same network. This thesis project reviews the security of the IEEE 802.11 WLAN standard and analyses a certain type of wireless attack called the Person-in-Middle (PiM) attack. The goal of this thesis project is to design solutions for the PiM attack to increase the overall security of the WLAN environment. The four proposed solutions to the PiM attack are Per-packet Authenticity and Integrity, Symmetric Authentication, Increasing Delay Time for Authentication, and Third Party PiM Attack Detector. Subsequent chapters of this thesis discuss these solutions.

1.1 - Problems with IEEE 802.11, the Wireless Network Standard

The Institute of Electrical and Electronics Engineers (IEEE) is a non-profit association that “aims to advance global prosperity by fostering technological innovation, enabling members' careers and promoting community world-wide” (IEEE Website). The IEEE standards are to unify hardware designs for technologies such as the Internet; IEEE 802.11 is one of the earliest WLAN standards defined.

The IEEE 802.11 standard has several known problems exploited. The standard is ‘weak’ in the sense that it does not provide data encryption for authentication nor association. Through authentication, computers are able to identify who they are, and through association, computers connect to an access point (AP), or a device that is physically connected to some outside networks. Without data encryption in the authentication data or association data sent, attackers can easily deceive access points to gain illegal access. Attackers may also generate a series of dis-authentication or dis-association messages to bring down the whole network [2].

1.2 - Method and Approach to Solve the Problem

One of the most straightforward approaches to fixing a poorly designed standard is to come up with newer standards. Currently there are several new standards deployed for WLANs. Although organizations can always invent new standards to counter existing flaws, the phase of converting from an older standard to a newer one will take a substantial amount of time. Currently the 802.11 and 802.11b standards are already widely deployed. Changing to a newer standard will require

hardware changes, adding cost to an organization that tries to adopt the newer standards. The approach that this thesis takes is to examine all the current and future standards. Other than reviewing the 802.11 standard, this thesis project also focuses on the PiM attack and the recommended solutions. The PiM attack is a very powerful and damaging Internet attack that is very difficult to counter.

This thesis project offers an introduction to WLAN standards, an overview of WLAN security, and an in depth analysis of the PiM attack. The impacts of this project will be concentrated on the social, economic, and ethical side.

1.3 – Social, Economic, and Ethical Impacts

This fundamental goal of this thesis project is to improve the WLAN Internet accessing environment by pointing out security flaws and suggesting solutions to them. Organizations that choose or have already chosen to deploy WLAN should consider the current existing problems.

The impact of this thesis will hopefully bring awareness to the community about the capabilities that a WLAN attacker may obtain. The project seeks to allow readers to perceive how attackers may undertake the attacks, and then analyzes each attack. The defense solution offered against some of the WLAN attacks will provide a more secure Internet accessing environment. The social benefits of this project are not limited to only providing a better and secure environment, but may also benefit the economy.

Every year companies lose a fair amount of money due to security breaches such as computer viruses and Internet attacks. The valuable data that companies store

on corporate databases, namely enterprise servers, may accumulate to several billions of dollars. This thesis project may provide another layer of protection to those data, impacting on the economy as a whole [3].

The rise in the field of Internet Security has also created business opportunities. The company Symantec, for example, bases their revenue on providing Internet security related services.

With the analysis provided by this thesis project, the expectation and the most desired situation is to discourage Internet attackers from performing any attacks. Organizations world wide have considered Internet attacking unethical and in several countries it is a violation of the law [4].

1.4 - Why Do We Need Wireless Network?

The major difference between WLAN and a normal local area network (LAN) is the ability that WLAN users have superior mobility. WLAN users may move with their laptops from place to place, yet still can obtain Internet Access. LAN users, on the other hand, are restrained to physical wires and the architecture of their buildings.

Disadvantages of WLANs as opposed to wired LANs are in WLAN's speed and security. WLANs have signals that are much easier to intercept (via air). WLANs also have a slower transmission rate, although this may not always be the case as newer versions of WLANs are comparable to LANs.

The questions arise: why do we need WLANs? Is mobility really a substantial issue? By deploying WLANs, organizations have sacrificed security for mobility. Although Internet Security problems with WLANs continue to emerge through time,

the deployment of WLANs has not decreased. “By 2006, research firm Gartner expects 99 million WiFi users and 89,000 public WiFi access points around the world.” [3] This proves the need and desire for a safer and a better WLAN environment.

This thesis project focuses on analyzing the IEEE 802.11 standard and the PiM attack. In chapter one of this document, I introduced the motivation behind this thesis project, the impacts upon completion, and the relevant Internet security literature. In chapter two, I give an overview of the IEEE 802.11 wireless local are network standard as well as the 802.11 family tree. Chapter three begins the real analysis of the 802.11 security. I discuss the basic security mechanisms that 802.11 provide such as the Media Access Control address lists to encryption and decryption methods. Finally in chapter four, I walk through the PiM attack and provided several solutions. The rest of the conclusion will concentrate on evaluating each of the attack solutions and determining which one is the best short term solution to the PiM attack.

Chapter Two: Introduction to IEEE 802.11 Wireless Local Area Network Standard

The IEEE organization developed the network standards to provide convenience to hardware vendors. The standardization of the Ethernet technology, or IEEE 802.2, that most of us use now created enormous commercial benefits. Products for the Ethernet technology ranges from connection cables to complex data forwarding devices called routers [5]. This chapter gives an overview of the IEEE 802.11 standard, its growth, and its current developments. The end of this chapter explains the IEEE 802.11 WLAN architecture that is most relevant to the analysis of the IEEE 802.11 in future chapters.

2.1 - The Growth of 802.11 Wireless Local Area Network Standard

Wireless communication has changed the way many things work. We have freed ourselves from the restraint of wires to a more mobile world with inventions such as cellular phones. As the demand for mobility grows, mobile communication as well as mobile data communication is also growing.

Mobile data communication continued to grow along with the personal computer revolution and the growth of the Internet. Laptops, personal digital assistants, desktop computers, and embedded computer systems are all designed to interconnect and exchange data. With this wide range of possible applications, a wireless data communication solution was necessary. The IEEE 802.11 and several other standards such as the General Packet Radio Service arouse around the same time. Over the years, the IEEE 802.11 standard emerged [6].

2.2 – The 802.11 Family Tree

The first standardization of LANs by IEEE was their Project 802. In 1980 the IEEE began meeting to discuss LAN standards and in 1990 IEEE formally approved the IEEE 802 standard. The IEEE 802 framework defines the physical and data link layers. The physical layer specifies the standard for the bit by bit transmission of data through the wires. The data link layer part defines the protocol for accessing the physical layer and how multiple-users should transmit data [7].

Following IEEE 802 comes the IEEE 802.3 and 802.2 standard. The Ethernet connection used today is another word for IEEE 802.3. IEEE 802.3 specifies a network access method using a technique called carrier sense multiple access with collision detection. This method ensures that when two or more computers are wired together in the same network, the transmission will take turns instead of colliding. The IEEE 802.2 standard provides a common method for establishing and maintaining a logical communication link without specific knowledge of the network access method or physical medium.

In 1997, the IEEE established its first standard for WLAN, IEEE 802.11. IEEE 802.11 was originally a logical extension from the IEEE 802 family. The IEEE 802.11 supports three wireless physical interfaces operating at speeds of 1 and 2 Mbps (Mega bits per second). IEEE 802.11 uses 2.4 GHz radio frequencies to transmit data [8].

2.3 - 802.11 Economics

Even after the initial publication of IEEE 802.11 in 1997, the market was slow

to commercialize WLAN systems. In fact, comparing the speed of 1 and 2 Mbps to fast Ethernets that can run up to 100 Mbps, no consumers preferred the WLAN.

WLAN picked up its sales in the year 2000 as most major computer, telecommunication equipment, and semiconductor manufacturers invested in the 802.11 market in some manner. Companies effectively reduced the component or hardware costs of WLAN, boosting WLAN sales. Seeing the potential of WLAN, companies like IBM, Dell, Intel, Microsoft, Texas Instruments, and Nokia have major investments in WLAN technology. By the end of year 2000, the IEEE 802.11 based WLANs have resulted in equipment sales of over $1 billion. In 2002 this amount rocketed to $3 billion [3].

2.4 - A Mobile Network Architecture

IEEE 802.11 defines a network architecture that enables WLAN equipments to be configured and connected in a variety of ways. In a WLAN, each end point is called a station. Stations may communicate with another directly or through a centralized distribution device called an access point. Access points relay messages from station to another, thus effectively doubling the wireless coverage. Its buffering capabilities allow power management for battery-powered devices, and its gateway functionality provides connectivity to a wired LAN or external network. An access point is interchangeable with the term “portal” [13]. The next two sections will describe two network infrastructures, the basic service set and the extended service set. Much focus will be concentrated on the security of the extended service set throughout this thesis project.

2.5 - Basic Service Set

The most simple type of configuration is called an infrastructure basic service set (BSS), depicted in figure 2.1.

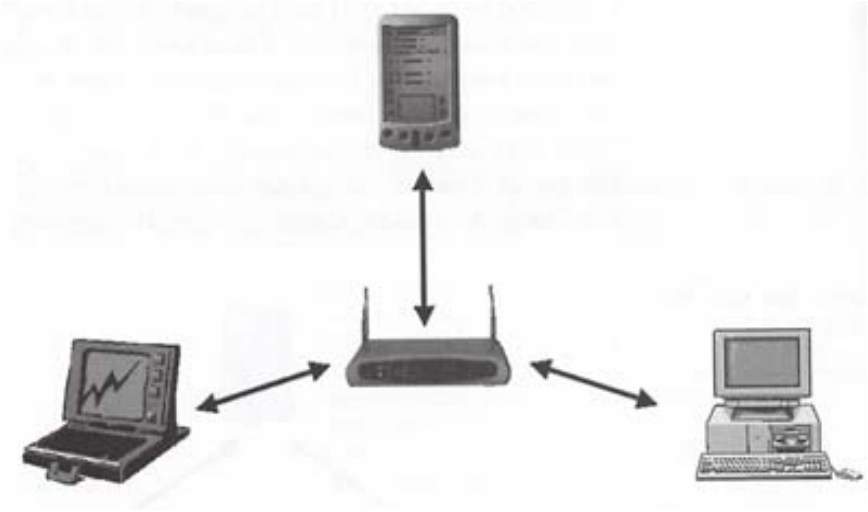

Figure 2.1 Basic service set architecture illustration [9]. The double pointed arrow indicates two-way communication between any of the devices. The access point is the device in the middle, connected wirelessly to a PDA, a laptop, and a desktop computer.

The access point in figure 1.1 is connected to three other devices: a Personal Digital Assistant, a desktop computer, and a laptop computer. The access point allows each of the connected devices to communicate between each other. Note that although all devices are capable of communicating wirelessly, they do not directly send data to each other. The access point is in charge of forwarding all data to the desired destination. A basic service set allows communication locally within the range of the same access point. A general purpose access point typically has a range of 200 meters.

2.6 - Extended service set

The basic service set in the above section allows communication within the local WLAN. For stations that wish to exchange data with another network, it needs an infrastructure called the extended service set, shown in to figure 2.2 below:

Figure 2.2 Extended service set architecture [9]. Three basic service sets shown here are connected to the distribution system (DS). The DS is a logical concept. It is independent of the media connecting an access point to another element of the distribution system.

An extended service set is merely a configuration with multiple basic service sets functioning as a single WLAN. An extended service set enables each access point within its local basic service set to determine if messages are to be sent to a station locally or remotely passed to another access point in another network. The distribution system in figure 1.2 is a logical concept, or a vague cloud that represent all other kinds of networks. For example, if computer A in basic service set one (BSS1) wishes to send a message to computer B in another basic service set, say BSS2. The access point in BSS1 will determine that computer B resides in another network and forwards it to the access point in BSS2 directly or through the distribution system. The message may be passed several times while it is in the

distribution system and reaches the access point in BSS2. The access point in BSS2 determines that it can forward the data to computer B directly. This concept of access points routing messages for stations is the mechanism used in IEEE 802.11. Extended service sets appear to be a single network to external entities, masking the mobility implied by a station's capability to move seamlessly between access points [9].

2.7 - Other Wireless Local Area Network Standards

IEEE 802.11 defines the architecture of an ESS and the basic services that enable the delivery of data over the distribution system; however; it does not specify how access points and portals should be implemented. This created problems, because hardware vendors came up with different access point implementations. IEEE 802.11 has other problems such as its access speed, which is apparently slower than the Ethernet. With such weaknesses in the standard, the IEEE formed other WLAN standards to address some of the problems in 802.11 [10].

IEEE published its 802.11a standard in 1999 to address the need for faster data transmission rates. Unlike 802.11, which uses 2.4 GHZ band, 802.11a specifies using the higher-frequency 5 GHZ band. IEEE 802.11a supports data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps [11].

Other standards to address speed and compatibility like the 802.11b also exist and IEEE has other future standards to improve WLAN. Figure 2.3 below is a list of WLAN related standards, including 802.11, which the IEEE has published or is actively creating [12]:

Name	Progress	Description
802.11	Completed	Wireless LAN PHY and MAC Specification (infrared and 2.4 GHz radio)
802.11a	Completed	Wireless LAN PHY and MAC Specification for the 5 GHz Radio Band
802.11b	Completed	Higher-Speed (5.5 and 11Mbps) WLAN PHY and MAC for 2.4 GHz Radio
802.11c	Completed	Bridge Operation with IEEE 802.11 MACs
802.11d	Completed	Extension to 802.11 for Operation in Additional Regulatory
802.11e	Active	MAC Quality of Service for Advanced Applications
802.11g	Active	Higher-Rate (20+ Mbps) Extensions in the 2.4 GHz band
802.11h	Active	Enhancements for Dynamic Channel Selection and Transmit Power Control
802.11i	Active	Enhancements for Security and Authentication

Figure 2.3 List of IEEE standards [12]. A list of IEEE completed standards and actively creating standards for the 802.11 family.

Chapter Three: Overview of Wireless Network Security

The IEEE 802.11 standard is IEEE's the first standard for WLAN. Currently network experts have identified this standard lack of any security mechanism. In the long term the IEEE has proposed other standards mentioned in chapter two to improve upon the wireless network security. In this chapter we discuss the initial security analysis of the IEEE 802.11 standard.

3.1 – The 802.11 Basic Security Mechanisms

The IEEE 802.11 standard specifies the Media Access Control (MAC) and physical (PHY) layers for devices capable of operation in the unlicensed band (2.4 and 5 GHz). In other words, the 802.11 standard provides a unified specification for the wireless devices that operate at the 2.5 and 5 GHz bands. The standard specifies operation at one of two modes: ad-hoc (Independent Basic Service Set) or infrastructure (Basic Service Set). In ad-hoc mode, stations may communicate directly with another station in their radio frequency range. In infrastructure mode, communication is via the access point. Each station sends packets to the access point which transmits to the destination station. This paper is only concerned with the security issues of the infrastructure mode, in which is currently the most widely used.

For a wireless station to obtain Internet access, it must establish a relation, or an association with the access point. Another relationship between the access point and a station is called authentication. Authentication acknowledges that the station is whom it claims to be. Complete association and authentication with an access point involves transition among three states:

1. Unauthenticated and unassociated
2. Authenticated and unassociated
3. Authenticated and associated

Management frames or data frames enable transition between the three states. For example, a station that just turned its power on initially starts at the unauthenticated and unassociated state. The station may shift to the authenticated and unassociated state by sending out an authentication management frame. Once the station and access point exchange authentication frames, the station transitions to the second state. Similarly if the station wishes to transition into the third authenticated and associated state, the station can exchange authentication management frames with the access point to complete the transition. At the third state, in other words, once authenticated and associated with the access point, the station is capable of exchanging data with the access point freely.

The primary methods for authentication and access control are open-system, shared-key authentication, and MAC-address based access-control lists. 802.11 also implements the Wired Equivalent Privacy Protocol (WEP) for encryption to provide confidentiality for the network traffic. However all of the above methods are insecure.

3.2 – MAC-Address Based Access-Control List

One mechanism that 802.11 provides to enhance association is the MAC address list. The MAC address list contains the MAC addresses or physical addresses of the wireless network interface cards. Each network interface card has its own

unique MAC address. The MAC address based access-control list in an access point contains a list of MAC addresses that are capable of associating with the access point.

It may appear that MAC address access-control list is a good way to determine which station is allowed to associate with a specific access point, given that MAC addresses are unique; however, because MAC addresses are also transmitted in clear text, MAC addresses are easy to discover with a sniffer. A sniffer is a type of software that captures radio signals and translates the captured signals into plain text. Once the attacker discovers the MAC address in the access-control list, the attacker can configure his own network interface card to the MAC address to gain access to the network.

3.3 – Wired Equivalent Protocol (WEP) Data Encryption

Once an access point has authenticated, associated, and granted access to the network to a station, the station can exchange data freely with the access point. The data being exchanged is transmitted via radio waves, and radio waves can potentially be sniffed and perceived easily. The WEP data encryption algorithm adds a layer of security by encrypting the data transmitted. The WEP algorithm uses the RC4 pseudorandom number generation algorithm originally developed in 1987 and licensed by RSA Data Security, Inc.

Figure 3.1 illustrates the WEP encryption process. The WEP algorithm takes a block of plaintext and bitwise XORs it with a pseudorandom key sequence generated by the algorithm to produce the ciphertext message to be transmitted. XOR is a binary bitwise operator yielding the result one if the two values are different and zero

otherwise. A ciphertext message is the encrypted message. To generate the pseudorandom key sequence, a secret key and initialization vector is used. The secret key is distributed among cooperating stations and is then concatenated with the initialization vector to generate a seed. The seed is then used as input to the pseudo random number generator (PRNG) and the PRNG finally outputs the key sequence. The key sequence generated from the PRNG is then XORed with the plaintext block concatenated with the integrity check value to produce the cipher text.

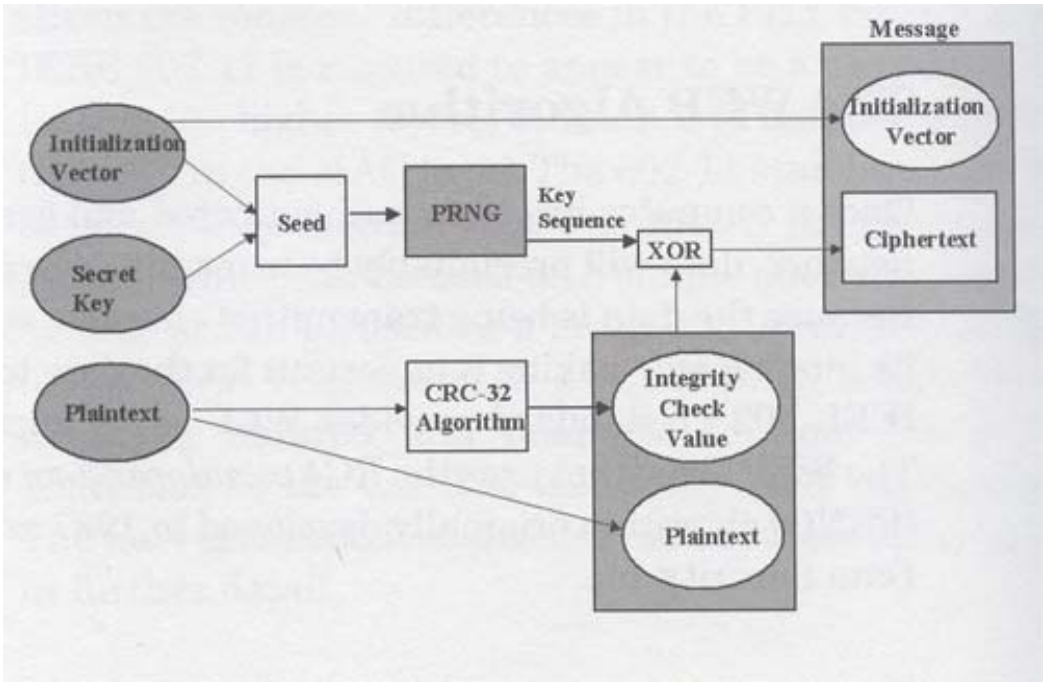

Figure 3.1 WEP Encryption [13]. The WEP encryption process starting with the plaintext, secret key, and the initialization vector to the final cipher text and generated frame. The act of concatenating the initialization vector, followed by the MAC protocol data unit, followed by the integrity check value generates the frame body.

The WEP decryption process is shown in figure 3.2. Once a message arrives, the initialization vector of the incoming message is combined with the secret keys to generate the seed that will be used in the PRNG operation. The WEP PRNG operation is then performed to produce the key sequence needed for decryption. Since the WEP algorithm uses a symmetric scheme in which the same key is used both the

encryption and decryption of data, the ciphertext received in the message is XORed to yield the original plaintext and integrity check value.

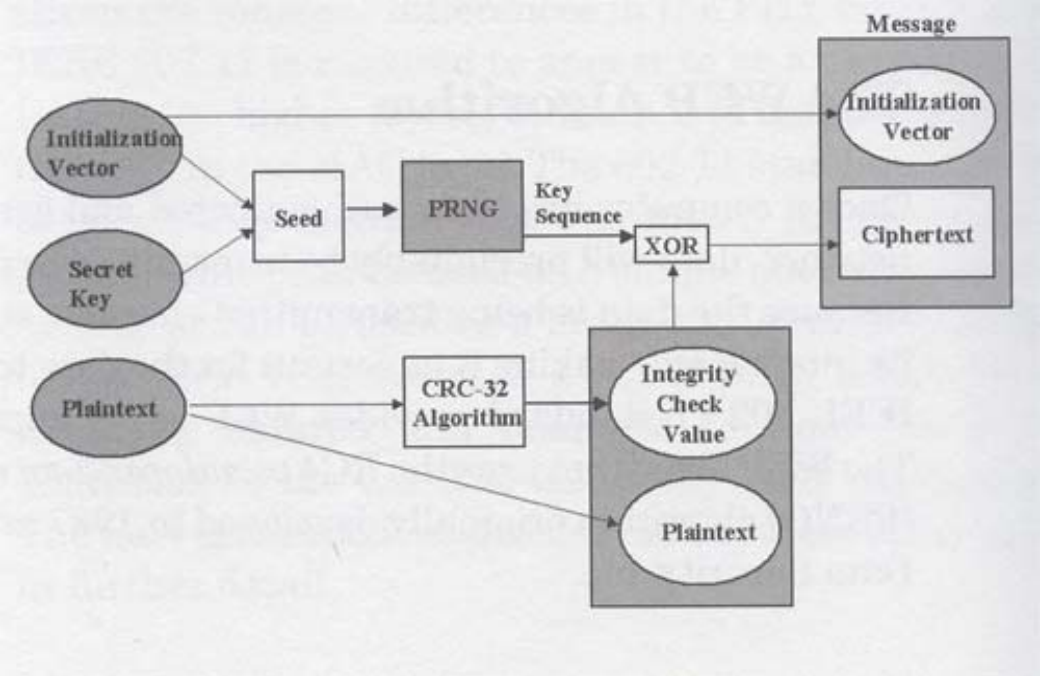

Figure 3.2 WEP Decryption [13]. The WEP encryption process starting with the plaintext, secret key, and the initialization vector to the final cipher text and generated frame. The act of concatenating the initialization vector, followed by the MAC protocol data unit, followed by the integrity check value generates the frame body.

In an 802.11 WLAN, if encryption is desired, the WEP algorithm is the only Wi-Fi-supported algorithm. The above example discussed the encryption and decryption process with a single key; however, the standard permits up to four secret keys. Other things should be noted about the WEP:

1. The WEP is optional. The delivered default is for WEP to be disabled.
2. The 802.11 standard relies on external key management services to distribute the secret keys to each station; however, the standard does not specify how these key distribution services should be implemented.
3. The secret keys under the control of the network administrator and remain static unless changed by the network administrator.

With the above properties of WEP, problems arise. First, the process of exchanging keys in a large network can be extremely time consuming due to the static nature of the keys and the manual process of key management. If a station is lost because of theft or accident, the system administrator will have to change the keys on all the stations. Finally, is the WEP encryption really all that safe? As discovered by three researchers[], WEP can be cracked by anyone with a sniffer, which is the name given to the hardware device or software that can capture data as it flies through the air. This basically means that all those companies that think they are securely using their wireless network are doing so under false pretenses.

3.4 – Services and Messages

In this section, we discuss the IEEE 802.11 specified services in more detail. The three basic security functions are authentication, integrity and confidentiality. The 802.11 standard includes specifications at the MAC and PHY levels to implement security through the use of authentication, association, and privacy services. The IEEE 802.11 standard specifies two categories of services in the MAC layer to accomplish the functionality of the distribution system. Every 802.11-conformant station must provide the authentication, deauthentication, privacy, and MAC service data unit delivery services. The distribution system must provide association, disassociation, distribution, integration, and re-association services. Out of the nine services specified by 802.11, three are used for controlling LAN access and confidentiality, and the other six are used for message delivery between stations.

Each service is supported by either management or data frames and by one or more MAC frame types.

The process of connecting a wireless station to a network begins with the station broadcasting probes containing the station MAC address and the basic service set identifier (BSSID) on all radio frequency channels used by 802.11. All access points within the radio range will respond with their own BSSID, MAC address, and the channel it operate on. The station can then limit its signal to the proper channel and begin the process of authentication.

The 802.11 standard provides two methods of authentication. In open system authentication, which may violate implicit assumptions made by higher network layers, a station can authenticate as long as the station receiving the request to authenticate does not decline, and the station passes any MAC address filtering rules that have been set up. Since WEP is delivered disabled by default, open system authentication is the default method and all authentication packets are transmitted without encryption.

The second method is shared key authentication. In shared key authentication, WEP must be enabled, and identical WEP keys must have been previously installed on the station and access point. The initiating station requests shared key authentication. The access point returns 128 bytes of randomly generated unencrypted challenge text. The initiating station then encrypts the text using the shared key and returns the WEP-encrypted data. The access point verifies the validity and integrity of the data, and then authenticates the connection and confirms the authentication with

the client. Successful completion of the process ensures that both stations secret keys match. After authentication is complete, the client initiates the association process.

In order for a message to be delivered, the distribution service must know which access point to access for each station. A station can only be associated with one access point at any given time. A mutually acceptable level of authentication must be established before association with an access point can be established and distribution system services can be obtained. The client transmits its BSSID, which is verified by the access point. With a positive match, the access point adds the client to its table of authenticated clients and returns an affirmation to the client. At this point, the client is now connected to the network. The process is shown in figure 3.3. Given the mobility of clients within the WLAN, a re-association service is also provided to facilitate the move from one access point to another within the extended service set. Recall that association and re-association are distribution system services.

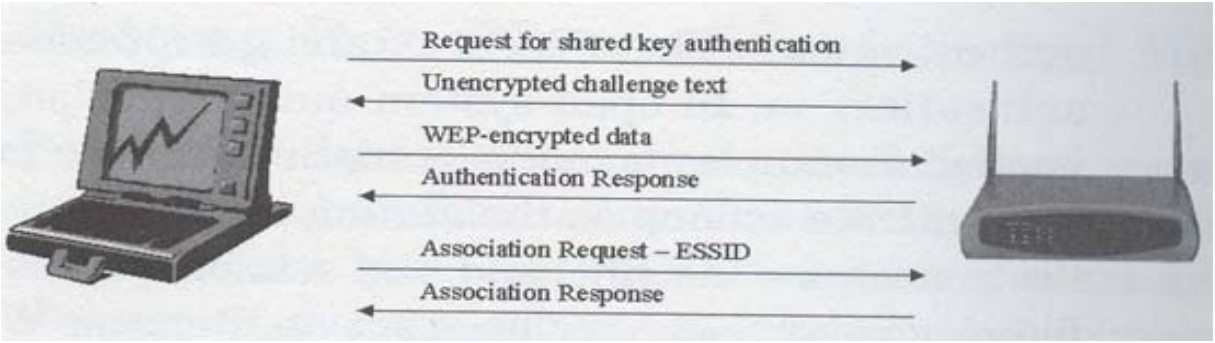

Figure 3.3 Authentication and Association Process[10]. The authentication and association process starts by the client sending a request for a shared key authentication. The authentication process completes when the client passes the unencrypted challenge text. The association process then starts with the client sending its ESSID. The whole process completes when the access point replies with the association response.

The deauthentication service is a station service just like the authentication service and is used to terminate an existing authentication. Deauthentication will also cause a station to be disassociated because association is a requirement for

authentication. Deauthentication is a notification, not a request, and may be initiated by either party (the station of the access point) and cannot be refused by either party. The last service is the privacy service, which is also a station service. The privacy service is used to invoke the use of the WEP encryption algorithm and encrypt the packets transmitted [14].

In this section we have discussed wireless security in general and some of its shortcomings. In the next sections of the chapter we will discuss the 802.11 WLAN PiM attack and its solutions.

Chapter Four: Analyzing the Person-in-Middle Attack

The PiM attack is an attack where the attacker is able to read and modify at will the messages transmitted between two parties without letting either party discover that the attacker has done so. The attacker must be able to observe and intercept messages going between the two victims [15]. In the case of a PiM attack on 802.11 WLAN and for this thesis project, the PiM attack is performed on the basic service set architecture. The subsequent sections contain a thorough explaination of the PiM attack on a simple BSS architecture and some solutions that I came up with to counter this attack.

4.1 – PiM Attack Concept

As mentioned in chapter three, the primary design flaw in the IEEE 802.11 standard is its lack of mutual authentication of the client and the access point. According to the standard, the 802.11 state machine only provides for one-way authentication. The client is authenticated to the access point. In summary, the design flaws that contribute to the success of the PiM attack are:

1. 802.11 provides only one-way authentication.
2. The authentication messages are not authenticated using any keying material.
3. Association frames are unauthenticated.
4. By using undocumented mode of operation, arbitrary frames can be generated with commodity hardware.

Below is a diagram of the normal authentication and association process of a client and access point without the attacker interfering:

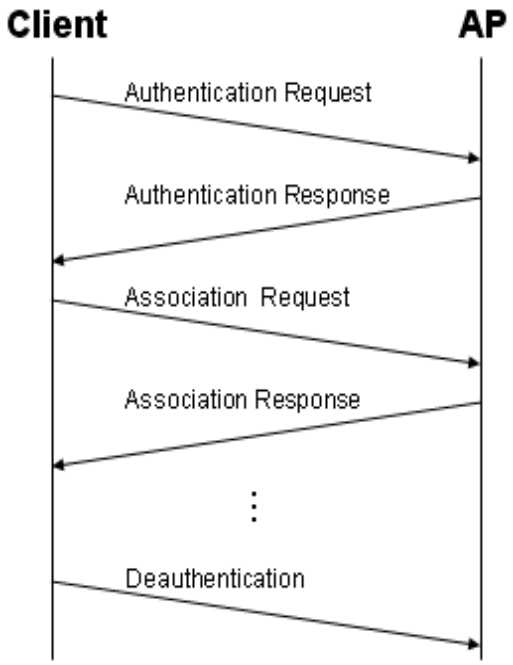

Figure 4.1 Graphical depiction of the normal authentication process (Created by Author). The Client begins by sending its authentication request to an access point. The omitted (…) part indicates data transferred. The deauthentication message at the end can go in both directions.

The client starts by locating the access point and sending an authentication request. The access point acknowledges the client with an authentication response. The one-way authentication flaw is very clear; the client does not need to authenticate the access point. Next the client sends out an association request to transition into the next state. The access point responds with an association response and the handshake is complete. The client then accesses the access point that may connect to other networks or the Internet. Upon terminating the connection, both the client and the access point can issue the deauthentication message. It is unimportant which party sends the message, the connection terminates as long as any party receives the deauthentication message.

Figure 4.1 illustrates another major 802.11 design flaw in which the client does not need to authenticate any messages. In other words, any user with a powerful enough wireless network interface card can generate the above messages and pretend to be a legitimate client. Attackers may also perform another type of attack called the Denial-of-Service attack where the attacker can generate a sequence of deauthentication or dissociation messages to devastate the network.

The next diagram depicts the attacker performing a PiM attack:

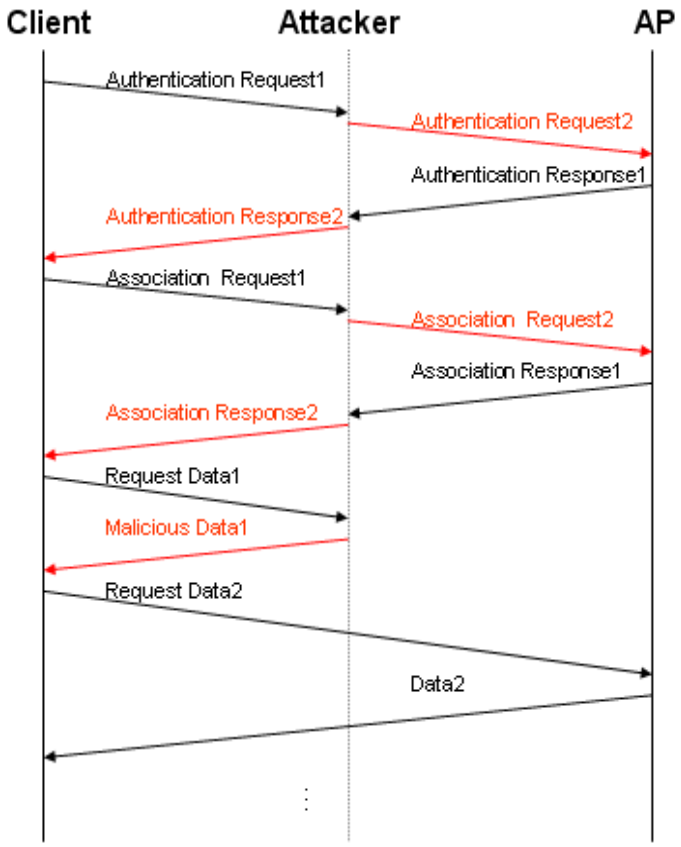

Figure 4.2 Graphical depiction of the PiM attack (Created by Author). Arrows marked in black are legitimate management messages. Arrows marked in red are messages generated by the attacker.

The client starts by sending an authentication request (Authentication Request1); however, the attacker intercepts this message. The attacker then generates its own authentication request (Authentication Request2 marked in red) and sends it to the

access point. The attacker generating this authentication message fools the access point that it is the client. The access point responds with an authentication response, which the attacker intercepts again. The attacker generates another authentication response (Authentication Response2 marked in red) to fool client that it is the access point. The procedure repeats for the disassociation message, where the attacker deceives both sides again. After the client receives the association response (Association Response2) from the attacker, the whole setup for the attacker is complete.

When the client sends out a request for Data1 (Data1 could be a request for a webpage or any file), the attacker in the above figure intercepts the message and replies with malicious Data1. Since the client does not have any idea of the existence of the attacker, it assumes Data1 is the right data it wants, and thus accepts it. When the client sends out a request for Data2, the attacker simply forwards the message for the client to the access point and vice versa. This is to show that the attacker does not need to modify every single message the client sends out.

The PiM attack illustrated above can cause a variety of damage, including fully controlling the client computer. In figure 4.2 above, the Malicious Data1 that the attacker generates and sends to client1 could range from a small computer virus to any Trojan software that gives the attacker control of the client computer. The client and the access point will have no way of detecting this attack under the current IEEE 802.11 standard.

4.2 – PiM Attack Solutions

As mentioned in the pervious section, in a PiM attack the attacker deceives both parties of a connection. This essentially avoids the access point and the client from detecting the attacker because the access point will authenticate the attacker and the client will think the attacker as the real access point (the client does not need to authenticate the access point). Detecting the attacker can be difficult; the PiM attack solutions will depend on stopping the attack before the attacker sets it up.

The first two solutions in the subsequent sections are gathered and derived from several research papers that I read [1] [2] [4]. The two solutions are initially ways to enhance 802.11 WLAN securities but after slight modification by myself, they can act as a counter to the PiM attack.

4.2.1 – Per-packet Authenticity and Integrity

The most straight forward solution is to directly deal with the 802.11 design flaws mentioned in the previous section. The lack of per-packet authenticity and integrity in IEEE 802.11 data and management frames is one of the primary contributors in many of the protocol's security problem. By providing per-packet authenticity and integrity, the attacker will no longer be able to forge messages that allow it to pretend the client nor the access point.

Per-packet authenticity and integrity can be achieved through a public and private key encryption technique. Each party holds two keys, a private key that is not shared with any other, and a public key that is well known. For each packet that the client or the access point transmits, both parties encrypt the packet with their own

private key to ensure authenticity and integrity and then decode the packet with the other's public key. This way, the attacker is not able to intercept traffic between the client and the access point, since the attacker does not know the private keys of any party and thus can not decode the transmitted packets.

4.2.2 – Symmetric Authentication

The PiM attack makes the client and the access point in a WLAN somewhat untrusted entities. The 802.11 standard lacks a symmetric (mutual) authentication scheme, where the client and the access point acknowledge each other. Once IEEE incorporates a symmetric authentication into the standard, it will hinder the attacker forging the access point. One suggestion for the access point would be to use a per-access point based shared secret key to avoid the attacker further intercepting the authentication message that the access point send out to its clients. The attacker can no longer read messages transmitted by the access point. If the attacker persists with the attack, the attack will most likely fail since the client will know which the legitimate access point is. The attacker will have no way of authenticating the access point as well as being authenticated since it does not know the shared secret key.

4.2.3 – Increasing Delay Time for Authentication

The access point sends out the authentication response once it acknowledges the client. 802.11 provides a MAC address based access control list for authentication. Since the attacker already intercepted the client's authentication request, it must know

the client's MAC address and thus can fake this authentication message easily. Once the access point acknowledges the client, it sends out the authentication response without delay. Increasing the delay time for authentication means having the access point wait for a longer period of time before sending out the authentication message to the client. In other words, increasing the time delay from the point where the access point receives the authentication request to the time the access point sends the authentication response out.

The reason of increasing the delay time is to allow the access point more time to detect whether the same authentication request is received more than once. In the wireless scenario, although the attacker intercepts the client's message, the radio signals of the client's authentication message will still reach the access point. The attacker's fake authentication message will be the second authentication request that the access point will receive. Instead of responding to both authentication messages (which is most probably what will happen), the access point will delay its response time and if the access point detects 2 authentication messages with the same MAC address within that time frame, it will deduce the possible existence of a PiM attacker.

Although it may be that both signals are sent by the client, in which the first signal faded for whatever reason, the action that the access point should take upon receiving two authentication messages is to time out for a longer time before re-authenticating the client. Every time the access point receives two authentication requests from the same MAC address it will time out. This approach may effectively stop PiM attackers since only one of the three cases will occur:

1. The access point receives no authentication message and takes no action.

2. The access point receives only 1 authentication message within the extended time frame then authenticates the client.
3. The access point receives more than 1 authentication message within the extended time frame and times out with no response.

The attacker will never receive authentication under the circumstances described above. So far the solutions mentioned are the ones that I have modified from existing methods. Finally, the next section explains the last short term low cost solution that I came up with.

4.2.4 – Third Party PiM Attack Detector

Another low cost solution is to add in a third party PiM attack detector. A third party PiM attack detector is simply a wireless capable computer sitting in the range of the access point. The PiM attack detector's job is to observe all data and management frames received and sent in the whole network. In one sense, the PiM attack detector is intercepting data in order to stop the PiM attack.

Assume that the attacker and the client are in the range of the access point as well as the PiM attack detector. The PiM attack detector first examines the number of authentication messages with the same MAC address exchanged. Comparing the normal authentication process with an attack, the number of authentication messages doubles from four to eight. Once the PiM attack detector observes this phenomenon, it can assume that an attacker exists in the WLAN and issue messages to inform the access point to take action. The access point can either issue deauthentication messages to the user with the MAC address, or it can try to locate the user.

The advantage of having a third party detector analyze of the network is:

1. It reduces the load of the access point.
2. It does not require any modification in hardware nor any protocols.
3. Easy to implement, only require programming an additional software for intercepting and analyzing management frames.

Chapter Five: Conclusion

The four PiM attack solutions proposed are:

1. Per-packet Authenticity and Integrity
2. Symmetric Authentication
3. Increasing Delay Time for Authentication
4. Third Party PiM Attack Detector

Both Per-packet the Authenticity and Integrity and Symmetric Authentication solutions suggested above are add-ons to the 802.11 standard. To implement such solutions will require IEEE changing the standard. The symmetric authentication solution involves further modification to the access point infrastructure. Currently 802.11 capable access points do not have a two way authentication model. Implementing this model requires the design and distribution of a new access point hardware which may appear costly in the long term.

The Increasing Delay Time for Authentication solution on the other hand may be a better approach to solve the PiM attack problem. Increasing Delay Time for Authentication requires changing a small part of the access point infrastructure. Although hardware vendors may still have to distribute the new access point after modification, it is still less costly and a better solution than the Symmetric Authentication solution.

The best solution appears to be the Third Party PiM Attack Detector. The PiM Attack Detector does not require any modification in the 802.11 standard nor any change in the WLAN hardware. The only costs to this solution reside in adding a third party computer and in the implementation of the analysis software. In terms of

cost and time to implement, the Third Party PiM Attack Detector is definitely the best choice.

5.1 – Interpretation of the Thesis Project

This thesis project is essential for wireless network users to obtain a higher security. The 802.11 standard may become more secure to the extent of detecting PiM attacks and defending it. The economic benefits can be significant, since 802.11 wireless technology will become more trustworthy and thus enabling the consumer market to grow further.

Since this thesis project focuses on design and analysis rather than implementation, there are no test results. The project achieved its goal of

1. Conceptually illustrating the PiM attack on an 802.11 WLAN.
2. Showing examples of the damage PiM attacks can perform.
3. Discussing several weaknesses of the 802.11 standard.
4. Providing a lost cost solution to this attack.

The next section describes the future recommendations for successors on this topic.

5.2 – Future Recommendations

This thesis project gives readers a more clear understanding of the flaws in the IEEE 802.11 standard and introduces the dreadful PiM attack. By far, the solutions provided by this thesis are all conceptual and have yet to be tested. For future recommendations, I suggest successors of this thesis project actually implement the

attack and prove the solutions effective. Successors may also think of ways that the attacker can take to counter the solutions proposed. It is certain that in the field of Internet Security, attacks co-evolve with their counters.

Works Cited

[1] Arbaugh, W.A., Shankar, N., Wang. J., and Zhang, K. Your 802.11 Network has No Clothes. Suntec City, Singapore. <http://citeseer.nj.nec.com/566520.html.>

[2] Bellardo, J. and Savage, S. (August 2003). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. Unpublished talk from University of California at San Diego. <http://www.cs.ucsd.edu/users/savage/papers/UsenixSec03.pdf>

[3] Legon, Jeordan (March 2003). Get ready to tune in to wireless Net. CNN News. <http://www.cnn.com/2003/TECH/ptech/03/12/ wifi.growth/index.html>

[4] Bing, Benny (2000). Performance Analysis. Broadband Wireless Access. Boston, MA: Kluwer Academic Pub.

[5] Asunción, Santamaría (2001). The Need for Standardization. Wireless LAN Standards and Applications. Boston, MA: Artech House.

[6] Asunción, Santamaría (2001). Future Trends. Wireless LAN Standards and Applications. Boston, MA: Artech House.

[7] Held, Gilbert (2001). Wireless LANs. Data Over Wireless Networks : Bluetooth, WAP, and Wireless LANS. NY: McGraw-Hill.

[8] Forouzan, Behrouz A (2003). Underlying Technologies. TCP/IP Protocol Suite. Boston, MA: McGraw-Hill.

[9] O'Hara, Bob (1999). The IEEE 802.11 Handbook: A Designer's Companion. NY: Standards Information Network, IEEE Press.

[10] Irvine, James (2002). Communication Systems. Data Communications and Networks: An Engineering Approach. NY: Wiley.

[11] Peterson, Larry L. (2000). The Physical Layer. Computer Networks: A Systems Approach. CA: Morgan Kaufmann Publishers.

[12] Asunción, Santamaría (2001). The Need for Standardization. Wireless LAN Standards and Applications. Boston, MA: Artech House.

[13] Irvine, James (2002). The Security Perspective. Data Communications and Networks : An engineering approach. NY: Wiley.

[14] Potter, Bruce (2003). 802.11 Security, CA: O'Reilly.

[15] Online Dictionary (March 2004). Person-in-Middle attack definition . <http://en.wikipedia.org/>

Bibilography

Alesso, H. P. (2002). The Intelligent Wireless Web. Boston, MA: Addison-Wesley.

Arbaugh, W.A., Shankar, N., Wang. J., and Zhang, K. Your 802.11 Network has No Clothes. In First IEEE International Conference on Wireless LANs and Home Networks, Suntec City, Singapore, December 2001.

Asunción, Santamaría (2001). Wireless LAN Standards and Applications. Boston, MA: Artech House.

Bellardo, J. and Savage, S. (August 2003). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. Unpublished talk from University of California at San Diego.

Bing, Benny (2000). Broadband Wireless Access. Boston, MA: Kluwer Academic Pub.

Borisov, N., Goldberg , I., and Wagner, D. Intercepting Mobile Communications: The Insecurity of 802.11. In Seventh Annual International Conference on Mobile Computing and Networking. Rome, Italy, July 2001. Retrieved August 2003 from the World Wide Web http://citeseer.nj.nec.com/476592.html.

Bray, Jennifer (2001). Bluetooth : Connect Without Cables, NJ: Prentice Hall.

Forouzan, Behrouz A. (2003). TCP/IP Protocol Suite. Boston, MA: McGraw-Hill.

Held, Gilbert (2001). Data Over Wireless Networks : Bluetooth, WAP, and Wireless LANS. NY: McGraw-Hill.

Irvine, James (2002). Data Communications and Networks : An Engineering Approach, NY: Wiley.

Legon, Jeordan (March 2003). Get ready to tune in to wireless Net. CNN News. Retrieved March 20, 2004 from http://www.cnn.com/2003/TECH/ptech/03/12/wifi.growth/index.html.

Loshin, Peter (2003). TCP/IP Clearly Explained. Boston, MA: Morgan Kaufmann.

O'Hara, Bob (1999). The IEEE 802.11 Handbook : A Designer's Companion. NY: Standards Information Network, IEEE Press.

Peterson, Larry L. (2000). Computer Networks: A Systems Approach. CA: Morgan Kaufmann Publishers.

Potter, Bruce (2003). 802.11 Security. CA: O'Reilly.

Stallings, William (2002). Wireless Communications and Networks, NJ: Prentice Hall.