SNMP Vulnerability Analysis and Suggested Countermeasures for Wireless Networks

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Software Engineering

by:
Harpreet Kaur Bindra
(8053111)

Under the supervision of
Dr. Maninder Singh
Assistant Professor

MAY 2007

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"SNMP Vulnerability Analysis and Suggested Countermeasures for Wireless Networks"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my research work carried out under the supervision of Dr. Maninder Singh.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(***Harpreet Kaur Bindra)***

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Maninder Singh)
Supervisor
Computer Science and Engineering Department
Thapar University
Patiala

Countersigned by

(Dr.(Mrs.) Seema Bawa)
Professor & Head
Computer Science & Engineering Department
Thapar University
Patiala

(Dr. R.K. Sharma)
Dean, Academic Affairs
Thapar University
Patiala

ACKNOWLEDGEMENT

Many people have been a part of my post- graduate education as teachers and friends. Here, I want to take the opportunity to thank them all.

First of all, I am deeply indebted to my supervisor Dr. Maninder Singh, Assistant Professor, Computer Science & Engineering Department, Thapar University, Patiala whose help, stimulating suggestions and encouragement helped me in all the time of research for and writing of this thesis.

I also want to extend my thanks to Dr (Mrs) Seema Bawa, Professor & Head**,** Computer Science and Engineering Department, Thapar University, Patiala and the entire faculty members for their excellent guidance and encouragement right from the beginning of this course.

I would also like to gratefully acknowledge the support of Yugma Kumar Agrawal and Manmeet Singh. I want to thank them for all their help, support, interest and valuable hints.

Most of all, I would like to thank my family, and especially my parents, for their endless love and support.

Harpreet Kaur Bindra

(8053111)

ABSTRACT

Securing any network infrastructure is like securing possible entry points of attacks on a country by deploying appropriate defense. Network security is an ongoing process that helps keep unauthorized parties from gaining access to the network. Any networked system where security or privacy protection of assets is valued needs security experts to protect and control it.

Wireless technologies represent a rapidly emerging area of growth and importance for providing ubiquitous access to the network for all of the user community. Because of great convenience and flexibility provided by wireless networks, the popularity of wireless networks has surged dramatically over the recent few years. Recently, industry has made significant progress in resolving some constraints to the widespread adoption of wireless technologies. Some of the constraints have included disparate standards, low bandwidth, and high infrastructure and service cost. Wireless is being adopted for many new applications: to connect computers, to allow remote monitoring and data acquisition, to provide access control and security, and to provide a solution for environments where wires may not be the best solution.

The increasing popularity of wireless networks has opened organizations up to new security threats and many traditional countermeasures are ineffective in dealing with them. Though wireless networks offer great benefits, they are more susceptible to attacks and require more protection than their wired counterpart. The fundamentals of network security remain the same in wireless networks also; it is still based on the three A's:

- Authentication of users, also known as access control.
- Authorization for access to network services and domains.
- Accounting of network activity, also known as auditing.

In wireless networks, data is broadcast in the open air, and it is impossible to have physical controls over the transmission boundaries. That makes eavesdropping or active attacks more easier than in wired networks, and hence security becomes the major concern in wireless networking. Since deployment of wireless network technologies in public places bears the danger of unauthorized users gaining access to network services, it is extremely crucial to be able to restrict access to the network only to authorized users.

An attack on a wireless network is an attempt to exploit a particular vulnerability or number of vulnerabilities that exist in it. Therefore, there is a great need to incorporate security in wireless networks. In order to make the wireless network secure, the vulnerabilities present in it need to be identified so that the security problems can be resolved before they can be exploited. One such vulnerability arises due to the Simple Network Management Protocol (SNMP) used to manage the network devices.

As SNMP is the most widely used network management protocol, it is natural to adopt SNMP-based management solutions for WLANs. SNMP is a request-response protocol that collects management information from network devices and provides a way to set and monitor configuration parameters in a wireless network. This enables the automatic reporting of access point faults to remote IP addresses, together with remote configuration over the network. Like many network protocols, SNMP has some associated vulnerabilities. This work investigates the behavior of SNMP in wireless networks and highlights the issues of information security due to the SNMP vulnerabilities present in the wireless networks.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 NETWORKS

Networks are widely used in both the business and consumer landscapes. A network involves a number of devices linked together to form a communications system for information and device sharing. Local Area Networks (LANs) are small, limited to about 500 meters, and are commonly deployed in corporate offices to facilitate low–cost, high–bandwidth information transfer within a company. Cities and other metropolitan regions can be connected via Metropolitan Area Networks or (MANs), and Wide Area Networks (WANs) involve systems communicating across large geographic regions such as states or countries. Globally, computers in networks interlink to form what is referred to as "the Internet."

Networks can be classified on many different bases like network layer (OSI, TCP/IP), scale (PAN, LAN, MAN, WAN), functional relationship (Client-Server, Peer to peer), topology (Bus, Star, Ring, Mesh) etc. On the basis of connection method, networks can be classified according to the technology used to connect the individual devices in the network that gives rise to **Wired** or **Wireless** networks.

1.1.1 Wired Networks

Wired networks are the most commonly used networks all over the world. Wired LANs use Ethernet cables and network adapters. Although two computers can be directly wired to each other using a crossover cable, wired LANs generally also need central devices like hubs, switches, or routers to accommodate more computers.

For dial-up connections to the Internet, the computer hosting the modem must run Internet Connection Sharing or similar software to share the connection with all other computers on the LAN. Broadband routers allow easier sharing of cable modem or DSL Internet connections, plus they often include built-in firewall support.

The installation of a Wired LANs involves Ethernet cables to be run from each computer to another computer or to the central device. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers are kept in different rooms. Ethernet cables, hubs and switches are very inexpensive. Broadband routers cost more, but these are optional components of a wired LAN, and their higher cost is offset by the benefit of easier installation and built-in security features. Ethernet cables, hubs and switches are extremely reliable, mainly because manufacturers have continually improved Ethernet technology for the past twenty years. Loose cables likely remain the single most common and annoying source of failure in a wired network [1].

1.1.2 Wireless Networks

Over the past few years, an evolution has taken place toward using networks wirelessly. As a result, the world has become increasingly mobile. In fact, today wireless interfaces are available to utilize network services that allow the people to use e-mail and access applications, and browse the Internet from just about anywhere. These wireless applications are enabling people to extend their workplace in a way that results in significant benefits. Wireless networks provide a great deal of convenience and flexibility, and are relatively easy to set up.

While the term wireless network may technically be used to refer to *any* type of network that is wireless, the term is most commonly used to refer to a telecommunications network whose interconnections between nodes is implemented without the use of wires, such as a computer network (which is a type of telecommunications network). Wireless telecommunications networks are generally implemented with some type of information transmission system that uses electromagnetic waves, such as radio waves, for the carrier

and this implementation usually takes place at the physical level or "layer" of the network.

1.1.3 Examples of wireless technology at work

Cellular telephones

Perhaps one of the most well known examples of wireless technology in action is the cellular telephone. These instruments use radio waves to enable the operator to make phone calls from many locations world-wide. They can be used anywhere that there is a cellular telephone site to house the equipment that is required to transmit and receive the signal that is used to transfer both voice and data to and from these instruments.

Security systems

One common example of an operation or operations where the implementation of wireless technology may supplement or replace hard wired implementations is in security systems for homes or office buildings. The operations that are required (e.g., detecting whether a door or window is open or closed) may be implemented with the use of hard wired sensors or they may be implemented with the use of wireless sensors which are also equipped with some type of wireless transmitter (e.g., infrared, radio frequency, etc.) to transmit the information concerning the current state of the door or window.

Television remote control

Another example would be the use of a wireless remote control unit to replace the old hard-wired remote control units that were sometimes used in the television industry. Some televisions were previously manufactured with hard-wired remote controls, which plugged in to a receptacle or jack in the television whereas more modern televisions use wireless (generally infrared) remote control units.

There are many benefits of deploying wireless LANs, which can be summarized as the following:

- **Attractive price**—Deploying a wireless LAN can be cheaper than a wired LAN because there is no need for wires; simply hook up an access point, and it can provide service to multiple computers.
- **Mobility**—Boost user productivity with the convenience of allowing them to wirelessly connect to the network from any point within range of an access point.
- **Rapid and flexible deployment**—Quickly extend a wired network with the ease of attaching an access point to a high-speed network connection.
- **Application agnostic**—As an extension of the wired network, WLANs work with all existing applications. As discussed previously, the standard protocol is TCP/IP, which is supported over all forms of wireless.
- **Performance**—WLANs offer a high-speed connection that, while equal to Ethernet, is quickly passing it in speed.

The benefits of WLANs are being recognized by individuals and businesses alike; recently the Gartner Group predicted that by 2005, 50 percent of the Fortune 1000 companies will have extensively deployed wireless networks, and that by 2010, the majority of Fortune 2000 companies will depend on wireless technology to meet their business and networking needs.

1.2 OVERVIEW OF WIRELESS NETWORKS

Wireless networks provide the next step in utility and convenience for many industries. In general, wireless networks provide the power and freedom of mobility, with the setbacks of reduced speed and unpolished functions (as compared to wired networks). While wireless networks have existed for decades, only the recent boom of handheld and mobile devices has spurred the demand necessary to create robust networks. Thus, many new wireless technologies, hardware, protocols and standards are currently still in the developmental phase.

Wireless networking is used to meet a variety of needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To avoid obstacles such as physical structures, EMI, or RFI,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

Wireless communication involves:

- Radio frequency communication,
- Microwave communication, for example long-range line-of-sight via highly directional antennas, or short-range communication, or
- Infrared (IR) short-range communication, for example from remote controls or via IRDA,

1.3 TYPES OF WIRELESS NETWORKS.

Wireless networks operate on the same hierarchy as their wired counterparts; small networks of three or more devices are referred to as Wireless LANs (WLANs), while the global wireless network is referred to as the wireless Internet. Other basic types of wireless networks include the Wireless Personal Area Network (WPAN), the Wireless

Metropolitan Area Network (WMAN), and the Wireless Wide Area Network (WWAN)[2].

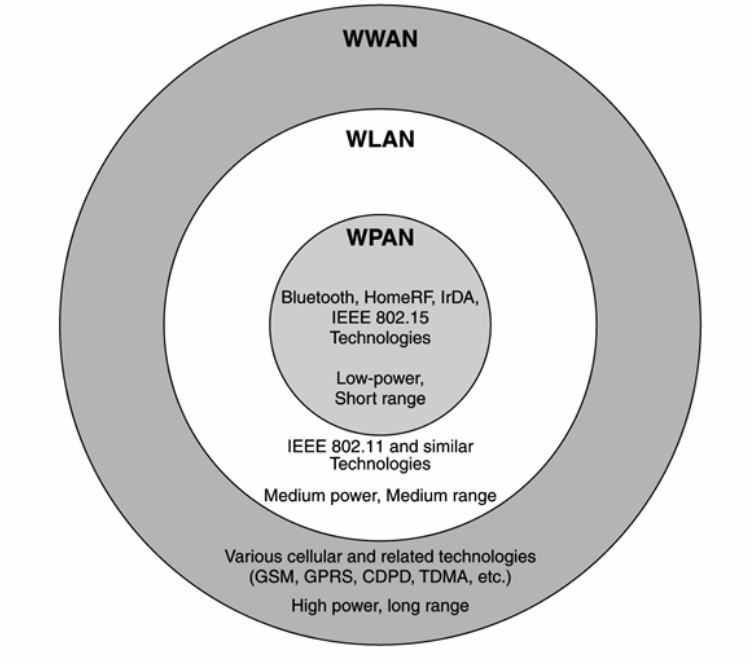

Figure 1.1: Types of Wireless Networks [3]

1.3.1 WPAN

A wireless PAN, for example, might involve some user wirelessly synchronizing his PDA to a laptop or desktop computer. Likewise, a wireless PAN can provide wireless connectivity to a printer. The benefit of eliminating the tangle of wires when using computer peripherals in this fashion is extremely useful, and the initial installation and movement of peripherals is easy. Example of WPAN: **Bluetooth**

Description**:** Bluetooth is a standard created with the support of many industry leaders who form the Bluetooth SIG (Special Interest Group). This specification provides for low-power, short-range connectivity between mobile devices (phones, computers, etc), and the Internet.

Features**:** Bluetooth is a short-range, ad hoc network that provides spontaneous connectivity. In WPANs, as devices move, the network moves.
Range: 20-350 feet (depending on whether the interaction is client-to-client or client-to-access point, and if the network is outdoors or in a building).
Transfer speeds: up to 1 mbps.

1.3.2 Wireless Local Area Network (WLAN)

Wireless LANs supply high performance within and around office buildings, factories, and homes. Users in these areas typically have laptops, PCs, and PDAs with large screens and processors that support higher-end applications. Wireless LANs efficiently satisfy connectivity requirements for these types of computer devices.

WLANs use electromagnetic waves (typically radio or infrared), to enable communication between devices in a limited area. Spread spectrum technology, based on radio transmission is most commonly used to deploy WLANs today.

Features: Unlike Bluetooth, WLANs provide continuous coverage for devices in the network. As devices may roam freely within the coverage areas, these coverage areas remain fixed.
Range: 100 – 500 feet indoors and up to 1000 feet outdoors.
Transfer speeds: up to 54 Mbps.

1.3.3 Wireless Wide Area Network (WWAN)

Wireless WANs offer mobile applications covering a large area, such as a country or continent. Because of economies of scale, a telecommunications operator can feasibly deploy the relatively expensive wireless WAN infrastructure to provide long-range connectivity for a large customer base. The costs such as deployment can be spread across many users, resulting in low subscriber fees.

Today's WWANs generally use digital cellular phone networks to enable notebooks and handheld computers to access the Internet across extensive geographic areas.

Features**:** Unlike WLANs, which are unlicensed and typically administered privately by the customer, WWANs are generally operated by public carriers, and use open standards such as AMPS, GSM, TDMA, and CDMA. Provides the greatest range but there are coverage holes and speed issues
Range: miles rather than feet.
Transfer speeds: from 5 kbps - 20 kbps.

1.4 WIRELESS NETWORK SYSTEM COMPONENTS

A wireless network consists of several components that support communications using radio or light waves propagating through an air medium. Some of these elements overlap with those of wired networks, but special consideration is necessary for all of these components when deploying a wireless network.

1.4.1 Users

A user can be anything that directly utilizes the wireless network. For example, a business traveler accessing the Internet from a public wireless LAN at an airport is a user. In some cases, however, the user might not be human. Because the wireless network exists to serve the user, the user is the component that receives the benefits of a wireless network. As a result, users are an important part of the wireless network. The user initiates and terminates use of a wireless network, making the term end-user appropriate. Typically, a user operates a computer device, which often performs a variety of application-specific functions in addition to offering an interface to the wireless network.

Users of wireless networks tend to be mobile, constantly moving throughout a facility, campus, or city. Mobility is one of the most prominent benefits of deploying a wireless network. For example, a person walking through a convention center while sending and receiving e-mail from a PDA is exercising mobility. The PDA in this case must have continual or frequent connections to a wireless network infrastructure.

Some users might require only portability; whereby, they stay at a particular location while using the wireless network for a specific period of time. An example of this type of usage is someone operating a laptop wirelessly from a conference room. The user will turn on the laptop after sitting down in the conference room and shut off the laptop before leaving. As a result, the wireless network doesn't need to support continual movement.

1.4.2 Computer Devices

Many types of computer devices, sometimes referred to as clients, operate on a wireless network. Some computer devices might be specifically designed for users, whereas some computer devices are end systems. In generally, any computer device might communicate with any other computer device on the same wireless network. Some of the computer devices for wireless networks are printers, laptops, desktop PCs, mobile phones, personal Digital Assistant (PDA).

1.4.3 NICs

The network interface card provides the interface between the computer device and the wireless network infrastructure. The NIC fits inside the computer device, but external network adaptors are available that plug in and remain outside the computer device.

Wireless network standards define how a wireless NIC operates. For example, a wireless LAN NIC might implement the IEEE 802.11b standard. In this case, the wireless NIC

will only be able to interface with a wireless network infrastructure that complies with the 802.11b standard. As a result, users must be careful to ensure that the wireless NIC they choose matches the type of wireless network infrastructure they want to access. Wireless NICs also comply with a specific form factor, which defines the physical and electrical bus interface that enables the card to communicate with the computer device.

1.4.4 Air Medium

Air provides a medium for the propagation of wireless communications signals, which is the heart of wireless networking. Air is the conduit by which information flows between computer devices and the wireless infrastructure. The communication through a wireless network can be thought of analogous to talking to someone. As persons move farther apart, it's more difficult to hear for them to each other, especially when a loud noise is present.

Wireless information signals also travel through the air, but they have special properties that enable propagation over relatively long distances. Wireless information signals cannot be heard by humans, so it's possible to amplify the signals to a higher level without disturbing human ears. The quality of transmission, however, depends on obstructions in the air that either lessen or scatter the strength and range of the signals.

1.5 IEEE 802.11: WIRELESS LAN STANDARD

WLAN products operate inside a collection of frequencies, known as a frequency band: 2.4 GHz for 802.11b/g and 5 GHz for 802.11a. To transmit data over radio waves, WLAN devices must superimpose the data being transmitted onto the radio wave, also known as a carrier wave because it carries data. This process is called modulation. Different modulation types exist and each has its benefits and tradeoffs in terms of efficiency and power requirements. DSSS modulations are used in 802.11b/g. OFDM

modulations are used in 802.11a/g. Together, the frequencies of operation and the modulation types define the Physical Layer (PHY) of the IEEE standard. Products are compatible at the PHY layer when they use the same frequencies and modulation. A second data layer, the Medium Access Control Layer (MAC) has been standardized across 802.11a, b and g shipped.

In 1999, the IEEE approved both the 802.11a and 802.11b standards [5]. 802.11a specified radios transmitting at 5 GHz and at speeds up to 54 Mbps using orthogonal frequency division multiplexing (OFDM) modulation technology. The 802.11b standard – now popularly known as Wireless Fidelity (Wi-Fi) –specified operation in the 2.4 GHz band (also known as the ISM band) and could achieve speeds up to 11 Mbps using direct sequence spread spectrum (DSSS) technology. Because DSSS is easier to implement than OFDM, 802.11b products appeared on the market first, starting in late 1999. Since then, 802.11b products have been widely deployed in universities, corporations, small offices/home offices (SOHO), in residential home and in public locations. It wasn't until early 2002 the first end-user products based on the 802.11a standard began shipment.

The IEEE 802.11a standard provides two key benefits over IEEE 802.11b. It increases the maximum speed per channel (from 11 Mbps to 54 Mbps) and increases the number of non-overlapping channels. The 5 GHz band is actually made up of three sub-bands, UNII1 (5.15-5.25 GHz), UNII2 (5.25-5.35 GHz) and UNII3 (5.725-5.825 GHz). Up to 8 non-overlapping channels are available when UNII1 and UNII2 are both used, versus 3 in the 2.4 GHz band. The total bandwidth available in the 5 GHz band is also higher than in the 2.4 GHz band – 83.5 MHz versus 300 MHz. Thus, an IEEE 802.11a-based WLAN system can support a larger number of simultaneous high-speed users without the potential for conflict.

These benefits come, however, with some tradeoffs in terms of compatibility and range. Because they operate in different frequency bands, IEEE 802.11a and IEEE 802.11b products are not compatible. A 2.4 GHz IEEE 802.11b access point, for example, won't work with a 5 GHz 802.11a network card [4].

Because of backward compatibility, an 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. It will be possible to upgrade the newer 802.11b access points to be 802.11g compliant via relatively easy firmware upgrades. Making 802.11g more attractive than 802.11a which would require installation of new wireless Access Points (AP) and radio cards.

Range at 54 Mbps will likely be less than existing 802.11b access points operating at 11 Mbps. As a result, the organizations don't count on upgrading the existing access points that currently provide 11 Mbps throughout all areas. Similar to 802.11b, 802.11g operates in the 2.4GHz band, and the transmitted signal uses approximately 30MHz, which is one third of the band. This limits the number of non-overlapping channels for 802.11g access points to three, which is the same as 802.11b. This means that the same difficulty with 802.11g channel assignment as with 802.11b when covering a large area where there is a high density of users. The solution ofcourse is to lower the power of each access point, which enables closer placement of access points.

Table 1: IEEE WLAN standards [6]

	802.11	**802.11a**	**802.11b**	**802.11g**
Standard Approved	July 1997	September 1999	September 1999	**June 2003**
Available Bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Frequencies of Operation	2.4 GHz DSSS, FHSS	5.25 GHz OFDM	2.4 GHz DSSS	2.4 GHz DSSS, OGDM
Number of Non-overlapping Channels	3	4	3	3
Data Rate per Channel	2,1 Mbps	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2, 1 Mbps
Compatibility	802.11	Wi-fi	Wi-fi	Wi-fi at 11 Mbps and below

1.6 WLAN ARCHITECTURE

An IEEE 802.11 WLAN is a group of stations (wireless nodes) located within a limited physical area. The IEEE 802.11 architecture consists of several components that interact to provide a WLAN that supports station mobility.

The basic building block of IEEE 802.11 LAN is the basic service set (BSS), which consists of some number of stations executing the same MAC protocol and competing for access to the same, shared wireless medium. The association between a station and a BSS is dynamic. When getting out of the range, a station may disassociate to the current BSS, and it may associate later to another BSS. The component that interconnects BSSs is the distribution system (DS). The DS can be a switch, a wired network, or a wireless network. A BSS connects to a DS through an Access Point (AP). An AP functions like a bridge, moving data between its BSS and the DS. A set of BSSs and the DS form an extended service set (ESS) network. Stations within an ESS may communicate and mobile stations may move from a BSS to another. The EES appears as a single logical LAN at the logical link control (LLC) level. The integration of IEEE 802.11 architecture with a traditional wired 802.x LAN is accomplished through a portal.

There are two types of WLANs: infrastructure-based WLANs and ad hoc WLANs. The vast majority of installations use infrastructure-based LANs.. In the infrastructure-based organization, a BSS contains a Point Coordinator (PC) station, which acts as a polling master that dictates the access to the wireless medium. Usually, the same station serves both as PC and as AP of a BSS.

An ad hoc wireless network is typically created in a spontaneous manner, for limited time duration and for a specific task. For example, in an organization, a group of employees participating in a meeting can organize their laptops in an ad hoc wireless network to facilitate communication and information exchange. Two stations in an ad hoc wireless network can communicate directly if the receiver is within the communication range of

the sender, or can use a multi-hop communication otherwise. Communication in an ad hoc wireless network is performed using a wireless routing protocol.

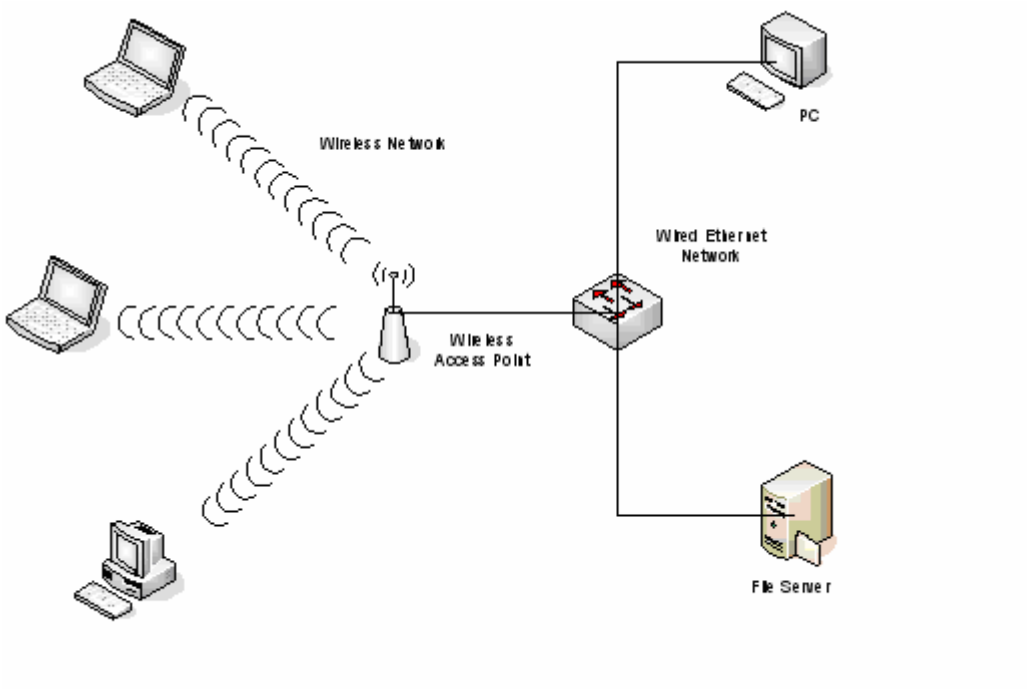

Figure 1.2 Infrastructure of WLAN

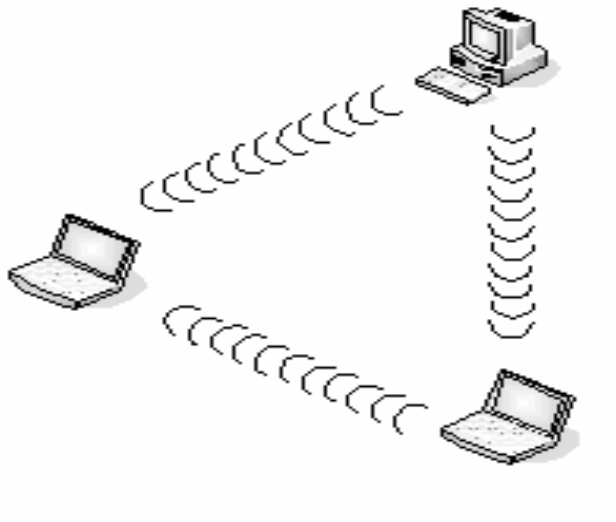

Figure 1.3 Ad Hoc WLAN

1.7 VULNERABILITY

To combat the network attacks, a network administrator needs the appropriate tools and knowledge to identify vulnerable systems and resolve their security problems before they can be exploited. A vulnerability is defined as “a weakness in a system allowing an attacker to violate the integrity, confidentiality, access control, availability, consistency or audit mechanism of the system or the data and applications it hosts.” (Wikipedia) This includes anything from a weak password on a router to an unpatched programming flaw in an exposed network service.

Security vulnerabilities exist not because of the technology or configuration implemented, but because the security policy does not address the issue or because users are not following the policy. For example, if a website is found to be susceptible to DoS attacks using ICMP traffic, the problem is found in the policy not addressing how ICMP traffic should be permitted into a network or, if it is addressed, the policy is not being followed. The true problem lies with all the malicious hackers out there just waiting to exploit these vulnerabilities and make the job and life more difficult. In order to better protect the systems, it helps to understand what an organization is up against

As compared to the number of vulnerabilities that are available against a wired network, a wireless network has many more and therefore requires more security procedures to defend against them. The simple fact that the medium of transmission is no longer contained in physically controllable wire opens up more possibilities for attacks to come from new directions. The most common threat to a wireless network is a hacker that can sit outside of the building and intercept network transmissions that leak from that building. This brings up one of the much vulnerability in the wireless networks that need to be addressed.

CHAPTER 2
A BRIEF REVIEW OF 802.11 STANDARD

IEEE 802.11 also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802). The term 802.11x [5] is also used to denote the set of amendments to the standard.

2.1 BASIC FEATURES OF IEEE 802.11 STANDARD

2.1.1 Stations and Access Points

A wireless network interface card (adapter) is a device, called a *station*, providing the network physical layer over a radio link to another station. An *access point* (AP) is a station that provides frame distribution service to stations associated with it. The AP itself is typically connected by wire to a LAN.

The station and AP each contain a network interface that has a Media Access Control (MAC) address, just as wired network cards do. This address is a world-wide-unique 48-bit number, assigned to it at the time of manufacture. The 48-bit address is often represented as a string of six octets separated by colons (e.g., 00:02:2D:17:B9:E8) or hyphens (e.g., 00-02-2D-17-B9-E8). While the MAC address as assigned by the manufacturer is printed on the device, the address can be changed in software.

Each AP has a 0 to 32 byte long Service Set Identifier (SSID) that is also commonly called a network name. The SSID is used to segment the airwaves for usage. If two

wireless networks are physically close, the SSIDs label the respective networks, and allow the components of one network to ignore tho0se of the other. SSIDs can also be mapped to virtual LANs; thus, some APs support multiple SSIDs. Unlike fully qualified host names (e.g., gamma.cs.wright.edu), SSIDs are not registered, and it is possible that two unrelated networks use the same SSID.

2.1.2 Channels

The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz. Neighboring channels are only 5 MHz apart. Two wireless networks using neighboring channels may interfere with each other.

2.1.3 Infrastructure and Ad Hoc Modes

A wireless network operates in one of two modes. In the *ad hoc* mode, each station is a peer to the other stations and communicates directly with other stations within the network. No AP is involved. All stations can send Beacon and Probe frames. The ad hoc mode stations form an Independent Basic Service Set (IBSS) [4].

A station in the *infrastructure* mode communicates only with an AP. Basic Service Set (BSS) is a set of stations that are logically associated with each other and controlled by a single AP. Together they operate as a fully connected wireless network. The BSSID is a 48-bit number of the same format as a MAC address. This field uniquely identifies each BSS. The value of this field is the MAC address of the AP.

2.1.4 Wired Equivalent Protocol

Wireless networks rely on an open medium, and the risk of using them is greatly increased if no cryptographic protection can be applied on the air link. With an open network medium, unprotected traffic can be seen by anybody with the right equipment. In the case of wireless LANs, the "right equipment" is a radio capable of receiving and decoding 802.11, which is hardly an expensive purchase. For extra eavesdropping power, a high-gain external antenna may be used.

2.1.5 Frames

Both the station and AP radiate and gather 802.11 frames as needed. The format of frames is illustrated below. Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection.

Octets: 2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Figure 2.1: An IEEE 802.11 Frame

There are three classes of frames. The management frames establish and maintain communications. These are of Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, Announcement traffic indication message, Disassociation, Authentication, Deauthentication types. The SSID is part of several of the management frames. Management messages are always sent in the clear, even when link encryption (WEP or WPA) is used, so the SSID is visible to anyone who can intercept these frames.

The control frames help in the delivery of data.

The data frames encapsulate the OSI Network Layer packets. These contain the source and destination MAC address, the BSSID, and the TCP/IP datagram. The payload part of the datagram is WEP-encrypted.

2.1.6 Authentication

Authentication is the process of proving identity of a station to another station or AP. In the open system authentication, all stations are authenticated without any checking. A station A sends an Authentication management frame that contains the identity of A, to station B. Station B replies with a frame that indicates recognition, addressed to A. In the closed network architecture, the stations must know the SSID of the AP in order to connect to the AP. The shared key authentication uses a standard challenge and response along with a shared secret key.

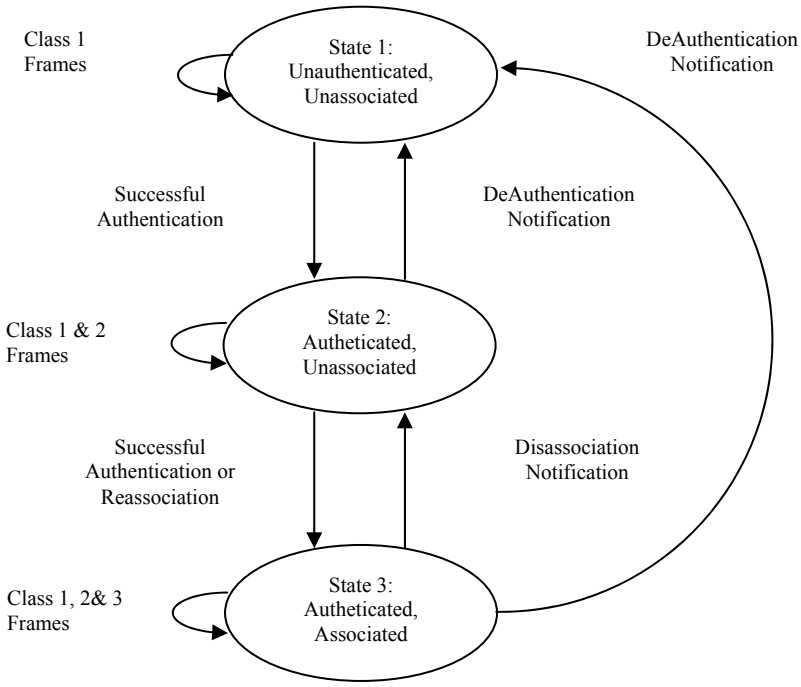

Figure 2.2: States and Services

2.1.7 Association

Data can be exchanged between the station and AP only after a station is associated with an AP in the infrastructure mode or with another station in the ad hoc mode. All the APs transmit Beacon frames a few times each second that contain the SSID, time, capabilities, supported rates, and other information. Stations can chose to associate with an AP based on the signal strength etc. of each AP. Stations can have a null SSID that is considered to match all SSIDs.

The association is a two-step process. A station that is currently unauthenticated and unassociated listens for Beacon frames. The station selects a BSS to join. The station and the AP mutually authenticate themselves by exchanging Authentication management frames. The client is now authenticated, but unassociated. In the second step, the station sends an Association Request frame, to which the AP responds with an Association Response frame that includes an Association ID to the station. The station is now authenticated and associated.

A station can be authenticated with several APs at the same time, but associated with at most one AP at any time. Association implies authentication. There is no state where a station is associated but not authenticated.

2.2 MANY FLAVOURS OF 802.11

The 802.11 standard [5] is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family:

- **802.11**—Pertains to wireless LANs and provides 1- or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a**—An extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
- **802.11b**—The 802.11 high rate Wi-Fi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- **802.11g**—Pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

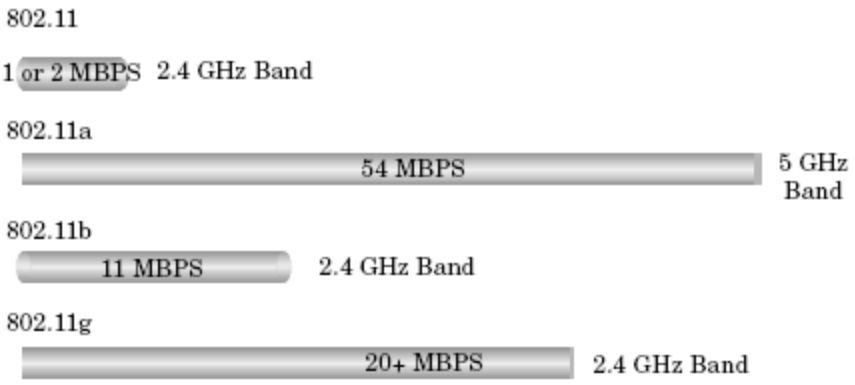

Figure 2.3: 802.11 Standards [8]

2.3 SECURITY IN IEEE 802.11

One issue with corporate wireless networks in general, and WLANs in particular, involves the need for security. Wireless networks have been notoriously insecure since

the early days of the 802.11b standard of the late 1990s. Since the standard's inception, major 802.11 weaknesses, such as physical security weaknesses, encryption flaws, and authentication problems, have been discovered. Wireless attacks have been on the rise ever since.

Applying strong wireless security mechanisms is the key to ensure that a wireless network is protected against unauthorized access and eavesdropping. Unfortunately, wireless security is vulnerable if implemented improperly.

2.3.1 WEP Weaknesses

The first, most basic level of securing a wireless LAN (WLAN) is to set up a wired equivalent privacy (WEP) [8] key. This is a means of encryption that encodes transmissions between an access point (AP) and client. This is a basic means of security, but it is not thorough. When wireless devices were first introduced, this was a quick and easy way to provide security. Unfortunately, WEP is inherently flawed; however, it might be the only option if the organization works with older equipment or client software [9].

If enough traffic is passed back and forth between client and AP, the packets can be intercepted and the encryption key deduced. This is not a likely issue for homes and small offices that have light wireless activity and uninteresting data. However, in an organization with high volumes of wireless traffic and critical data, it is easy for an intruder to crack the code. It is perhaps worth the effort of the intruder.

WEP is vulnerable to attack for several reasons:

- Distributing WEP keys manually is a time-intensive, laborious task. Because it is tedious to manually rekey the WEP code, the keys are not likely to change frequently. Therefore, an attacker probably has enough time to decipher the key.
- When keys are not changed often, attackers can compile so-called decryption dictionaries. These are huge collections of frames, encrypted with the same key. These frames can then be analyzed and used for attack.

- Standardized WEP implementations use 64- or 128-bit shared keys. Although the 128-bit key sounds excessively durable, it is still possible to crack a key this size within a short interval with sustained traffic.
- WEP uses RC4 for encryption. Of all the possible RC4 keys, the statistics for the first few bytes of output are nonrandom, which can provide information about the key.

2.3.2 IEEE 802.1X Authentication

The Institute of Electrical and Electronics Engineers (IEEE) 802.1X standard [13] is an improvement over the capabilities of the WEP. Although WEP provides encryption services, 802.1X provides authentication services. WEP offers a certain measure of encryption between AP and client; however, the data still floats in the ether, exposing it to analysis and examination. In a wired network, unauthorized devices can be blocked from the network if unused RJ-45 jacks are disabled and Media Access Control (MAC) addresses are associated to Ethernet switch ports.

Manage Port Access

WLANs can include or exclude devices based on MAC addresses using access control lists (ACLs). Although this type of ACL is easy to implement and manage on small networks, they are tough to manage in large and dynamic networks because individual MAC addresses have to be entered manually for each authorized device. Obviously, this is laborious.

Attacking with MAC

Because ACLs use MAC addresses, they are also prone to attack. An intruder can sit nearby and pick up traffic between the AP and authorized clients. Although the contents

of a WEP conversation are encrypted, the MAC address is not. As a result, an attacker can do one of two things:

- The patient attacker can wait until the monitored station disassociates from the network, and then simply reconfigure the network interface card (NIC) to broadcast the intercepted MAC address.
- The impatient attacker can simply send a disassociate request to the AP, bumping the legitimate station off the WLAN. Before the legitimate station can reassociate, the attacker can associate with the spoofed MAC address.

The LAN Port Access Control framework, outlined by the 802.1X standard, helps control access to one's WLAN.

2.3.3 802.1x Protocols

802.1X [13] can be thought of as a control inside the Ethernet switches and APs. The control starts in the OFF position. It considers 802.1X requests and if it decides to grant access, the control moves to the ON position. After a period of time, the station times out or disconnects, moving the control back to the OFF position.

Although the credibility of WEP has taken a beating, it's not totally out of the WLAN security game. WEP is a necessary part of an 802.1X deployment. WEP, used in conjunction with 802.1X, is far more secure than when it is used in static deployments. An even more robust security mechanism is the Wi-Fi Protected Access (WPA) [28]

There are several protocols used with the 802.1X standard for LAN Port Access Control. Within the 802.1X framework, a LAN station is not allowed to pass traffic through an Ethernet device or WLAN AP until it has successfully authenticated itself. After it has been authenticated, the client can pass traffic on the LAN.

There are 43 protocols that work within the framework of 802.1X authentication. Some of the popular protocols are covered in the sections that follow.

Extensible Authentication Protocol

The EAP is a framework that supports multiple methods of authentication. In essence, EAP manages the authentication, but the variant of EAP used dictates how clients are authenticated. Some authentication methods include:

- Token cards
- Kerberos
- Public key authentication
- Certificates
- Smart cards
- One-time passwords (OTP)

Several variations on EAP are possible. Depending on the organization's need, it allows different types of authentication.

As Figure 2.4 shows, EAP authentication is a multi-step process:

1. The client associates with the AP.
2. The AP blocks the client from accessing the network.
3. The client provides login information.
4. A Remote Authentication Dial-In User Service (RADIUS) server and client authenticate each other.
5. A RADIUS server and client agree on a WEP key.
6. Authentication is completed.

This is the basic framework of how EAP works. However, individual authentication methods can make the process slightly different.

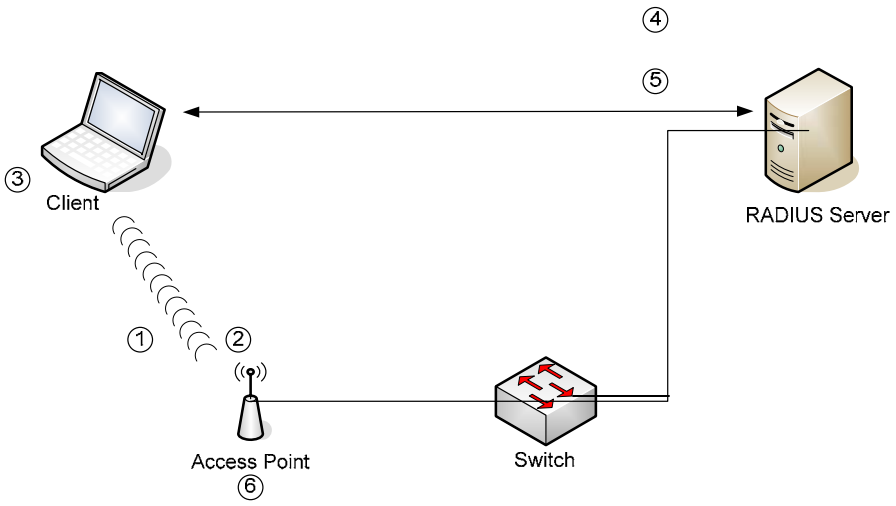

Figure 2.4. The EAP Authentication Process

EAP-TLS

EAP with Transport Layer Security (EAP-TLS) requires that both the station and RADIUS server authenticate themselves using public key cryptography, such as smart cards or digital certificates.

This conversation is secured with an encrypted TLS tunnel. That is, only the authentication is encrypted. After that is complete, then WEP, WPA, or WPA2 provide user data encryption. Although this makes EAP-TLS resistant to decryption dictionary and man-in-the-middle (MITM) attacks [29], the station's identity (and the name bound to the certificate) can still be culled by attackers.

Because EAP-TLS is standard on Microsoft Windows XP, Windows 2000, and Windows Server 2003, it is popular in Windows-based environments. Figure 2.5 shows EAP-TLS in action

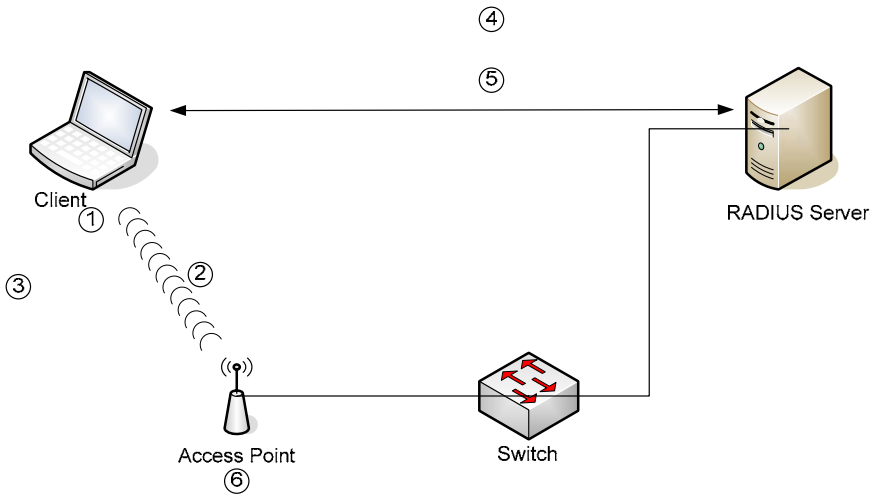

Figure 2.5: The EAP-TLS Authentication Process

The EAP-TLS authentication process is as follows:

1. The client associates with the AP.
2. The AP blocks the client from accessing the network.
3. The client authenticates the server with a certificate.
4. The RADIUS server authenticates the client with a certificate.
5. The RADIUS server and the client agree on a WEP key.
6. A secure tunnel is established between the client and the server.

The downside to this method is that issuing digital certificates to each station is time consuming, and most organizations prefer to use usernames and passwords for wireless authentication. Protected EAP (PEAP) is a good substitute for EAP-TLS.

Wi-Fi Protected Access (WPA)

Another means of WLAN security comes in the form of Wi-Fi Protected Access (WPA). WPA was introduced in 2003 by the Wi-Fi Alliance, a nonprofit association that certifies WLAN product interoperability based on IEEE 802.11 specifications. Two versions of WPA exist: WPA and WPA2. They are described below.

WPA

WPA was designed as a replacement for WEP. The Temporal Key Integrity Protocol (TKIP) is an improvement over WEP. It causes keys to automatically change, and when used in conjunction with a larger initialization vector (IV), it makes discovering keys highly unlikely.

On top of authentication and encryption improvements, WPA secures the payload better than in WEP. With WEP, cyclic redundancy checks (CRC) are used to ensure packet integrity. However, it is possible to alter the payload and update the message CRC without knowing the WEP key because the CRC is not encrypted. WPA uses message integrity checks (MIC) to ensure packet integrity. The MICs also employ a frame counter, which prevents replay attacks.

Breaking into a WLAN using WPA is more difficult than WEP because the IVs are larger, there are more keys in use, and there is a sturdier message verification system.

WPA2

WPA2 is the second and latest version of WPA.

The most important difference between the two is the method of encryption. WPA uses RC4, whereas WPA2 uses AES. Not only is the AES encryption method much stronger, it is also a requirement for some government and industry users.

WPA2 is backward compatible with WPA, and many WPA-certified products can be upgraded with software to WPA2. However, some products might require hardware upgrades. WPA was designed to be a software upgrade to WEP. However, WPA2 didn't have such a design goal. As such, in many cases a hardware upgrade will be necessary to update to WPA2.

2.3.4 Encryption

Scrambling a WLAN's data as it leaves the AP, and then unscrambling it when it arrives at the client, requires an encryption method. The popular RC4 has already been discussed, but sturdier, stronger encryption methods are out there and in use in WLAN systems, as described next.

Data Encryption Standard (DES)

Data Encryption Standard (DES) [10] is an encryption method that uses a secret key. It is so hard to break (it provides 72 quadrillion possible keys) that the U.S. government forbids its exportation to other countries. It is tough to break because the key is randomly chosen from an enormous pool.

DES applies a 56-bit key to each 64-bit block of data. This is considered strong encryption. Of course strong is a relative term, and if someone is really determined and has the resources, it is possible to crack DES. Many organizations employ triple DES, which applies three keys in succession.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) [11] is poised to become the de facto encryption standard. AES applies 128-, 192-, or 256-bit keys to 128-, 192-, or 256-bit blocks of data.

As of 2007, there had been no reported cracks of AES, and it is the first time that the U.S. Government's National Security Agency (NSA) authorized an encryption tool for transmission of top-secret, classified information.

CHAPTER 3

LITERATURE REVIEW

3.1 INTRODUCTION TO WIRELESS LAN SECURITY

The wireless industry has evolved phenomenally over the past few years. Wireless transmission (once the domain of amateur radio enthusiasts and the military) is now a commonplace method of data communication for cellular phones, wireless PDAs, text pagers, and, most important, wireless LANs (WLANs).

As there are a number of divergent technologies for wireless networks today (i.e., 802.11b, Bluetooth, etc.) most users standardize on one of these for their corporate networking needs. There are so many methods and forms of hacker attacks to steal corporate data that wireless measures designed for convenience can be exceedingly harmful without actually taking the proper measures.

Wireless networks are supported by having several transceivers scattered across the typical enterprise to blanket the corporate offices in a web of wireless transmission devices called access points. Access points (APs) are strategically placed in fixed locations throughout the company offices to function in tandem like cells of a cell phone network. They function together so that as the computer user moves from office to office, he is still covered by the reception of these wireless network routing devices.

3.2 FACTORS OF SECURITY

Primary factors that define security in a wireless environment can be boiled down to five elements; they are tightly integrated interdependent components.

3.2.1 Theft

Unauthorized users often try to log into a network to steal corporate data for profit. Employees who have been terminated often feel resentment and anger against their former employer. It is possible for some users to turn that anger into an attempt to steal corporate data before leaving their company. This is why the easiest type of security measure is simply to disable a user's account at the time of termination. This action is a good security measure and prevents the likelihood of account abuse during the transition out of the company.

3.2.2 Access Control

Does the company have a policy to set passwords for network shares? Do the network administrator knows who is sharing what, and with whom? Many companies set very simple access permissions. Some users want to share a document from one employee to another so they just share "Drive C" on the network. But if they don't remember to turn off the sharing, everyone within that network segment has full read and write permission to that user's Drive C. If there is a virus running across the network, then the user's computer is fully vulnerable and will most definitely be compromised. Wireless networks not only have all the same access control vulnerabilities as wired networks, but they can easily be accessed by outsiders.

The most common type of attack is simply to sit outside an office building and use a wireless network interface card to roam onto any available 802.11b network. Since the majority of users fail to set even the simplest access control barriers that prevent a

random user from accessing the network, everything on the network becomes vulnerable to attack, theft, or destruction from a virus.

3.2.3 Authentication

How to make sure that the user logged in is really that person? It is an all too common practice for people to use other people's accounts to authenticate themselves to the server. In most wireless networks, businesses often configure one account, "Wireless User," and that account can be used by several different devices. The problem is that a hacker (with his own wireless device) could easily log onto to this general account and gain access to the network.

To prevent an unauthorized user from authenticating himself into the network, the router can be set to permit only connections from authorized wireless network cards. Each wireless network card has a Media Access Control (MAC) address that uniquely identifies it. The router can be set to authenticate those wireless users with a network card that is pre-authenticated to use the network. This protects the network against users who are trying to gain access to the system by roaming around the perimeter of the building looking for good reception to log onto the local area network

3.2.4 Encryption

If a user is not able directly to log into the network, he may use a wireless "packet sniffer" to try and eavesdrop on the network traffic. In that way, even if the hacker is unable to authenticate himself onto the network, he can still steal sensitive corporate data by monitoring the traffic for usable information. In addition to viewing private data files, the hacker is potentially able to "sniff" usernames, passwords, and other private information to gain access onto the network. Wireless routers support medium and strong levels of encryption that scramble the data and make it unusable to anyone trying to eavesdrop on the network traffic. Only the users at either end of the "authorized" connection can view and use the data.

Unfortunately, most users don't turn on encryption in their wireless devices to protect themselves against eavesdropping! Most wireless routers have an internal Web site that allows for the very simple and easy configuration of data privacy. Wired equivalent privacy (WEP) [8] is a security protocol for wireless local area networks (WLANs) designated by the 802.11b standard. WEP offers a level of security similar to that of a wired LAN. Wired LANs offer greater security than WLANs because LANs offer the protection of being physically located in a building, whereas a wireless network inside a building cannot necessarily be protected from unauthorized access when no encryption is used. WLANs do not have the same physical confinements and are more vulnerable to hackers. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. WEP, used on both data link and physical layers, does not provide point-to-point security.

Most wireless routers offer 64- and 128-bit encryption with a user specified encryption key that scrambles the data according to the input. This key is needed at points to decode the data into a usable form. Most users, however, keep this option disabled and therefore are vulnerable to anyone intercepting network traffic or even roaming onto the network.

3.3 THE STATE OF WIRELESS LAN SECURITY

One issue with corporate wireless networks in general, and WLANs in particular, involves the need for security. Wireless networks have been notoriously insecure since the early days of the 802.11b standard of the late 1990s. Since the standard's inception, major 802.11 weaknesses, such as physical security weaknesses, encryption flaws, and authentication problems, have been discovered. Wireless attacks have been on the rise ever since.

To date, the list below includes some of the more salient threats and vulnerabilities of wireless systems:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an agency's computer or voice (IP telephony) network through wireless connections, potentially bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of Service (DoS) attacks [29] may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their physical movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to secretly gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use a third party, untrusted wireless network services to gain access to an agency's network resources.
- Internal attacks may be possible via ad hoc transmissions.

As with wired networks, agency officials need to be aware of liability issues for the loss of sensitive information or for any attacks launched from a compromised network.

Applying strong wireless security mechanisms is the key to ensure that a wireless network is protected against unauthorized access and eavesdropping. Unfortunately, wireless security is vulnerable if implemented improperly. The following sections examine some of the issues surrounding wireless security and how to avoid trouble.

There are real issues to consider when implementing a WLAN, therefore, it is important to focus on the integrated security features present within 802.11b [5] and their limitations. 802.11b offers features and functionality that provide the user with greater security in the wireless environment, however these security services are enabled for the most part through the wired equivalent privacy (WEP) mechanism to protect the network at the link level during wireless transmissions that take place between the client and the access point. However, WEP is not able to offer end-to-end security, but it does attempt to secure the actual radio transmission by encrypting the data channel.

3.3.1 Securing WLAN

The most important issue when dealing with wireless security is to consider the fundamental security mechanisms in the wireless network. There are two primary means of adding security to the wireless environment

Authentication—This mechanism has the objective of using WEP to enable the security to be verified by determining the actual information that defines each wireless workstation. It is necessary to yield access control to the network by restricting wireless workstation access to those clients who can properly authenticate themselves to the server.

Privacy—WEP maintains an effective level of privacy when dealing with security for the data communication channels in the wireless network. It attempts to stop information from being “hacked” by attackers trying to eavesdrop on the data transmissions. The

objective is to make certain that messages are not altered while moving from the wireless workstation to the access point or server. Essentially, this is the means that enables the user to trust this information so that one can be reasonably certain the information is secure and reliable.

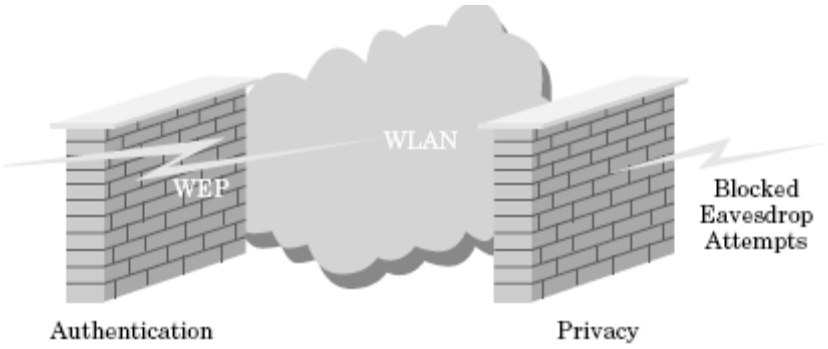

Figure 3.1 Securing WLAN [8].

3.3.2 Authenticating Data

When a wireless user attempts to acquire access to the wired network infrastructure, there are two ways in which access can be obtained:

Open system—Any user in range of the access point can roam onto the system (as long as the router is not set up to filter out the unique MAC address of wireless workstations that are not supposed to have access).

Encrypted system—All data is scrambled and access barriers are put into place so that a hacker cannot eavesdrop on that data.

In an open system without encryption, a wireless workstation can join the WLAN by using identity types of verification methods. The actual access request in an open environment occurs when the wireless server replies with the service set identifier (SSID)

for the WLAN. This means there isn't any actual authentication taking place; the wireless workstation simply roams onto the network.

Because of the unique SSID set for a company, many people believe that nobody could actually roam onto a network without knowing what unique identifier defined the network. In fact, it is possible for a wireless user to leave the SSID as "NULL" or blank; then when he is in range of the access point, the wireless workstation automatically finds and logs into the network. This means that basic systems of authentication are not sufficient to protect the network. This is why a combination of encryption and authentication is important in implementing the wireless security—but this still represents a small part of what needs to be done to provide a truly secure WLAN.

Client Authentication in a Closed System

When a wireless workstation replies to the access point with a null or empty string in place of the actual SSID, it is automatically authenticated into the open system. However, when working in a closed authentication environment, the wireless workstation must reply with the exact SSID in order to log into the wireless network. The client is only granted access if it replies with the exact SSID string that identifies the client to the server.

Shared Key Authentication

The shared key authentication encryption mechanism uses the "challenge- response" mechanism. The idea is that each wireless client has an understanding of what is commonly referred to as a "shared secret." The access point creates a random type of challenge that is transmitted to the wireless workstation. The wireless workstation then uses the encryption or WEP key it shares with the access point. The challenge is itself encrypted and then replies with the answer to the access point, which then deciphers that answer sent by the client. Based on the result, the client is granted access only if the deciphered answer is the same expected value as the random challenge [14].

RC4

Data is encrypted using the RC4 cipher [30]. Note that the wireless workstation does not authenticate the access point, so that there is no verifiable means to make certain that the client is effectively talking to an authorized access point on the WLAN. The problem is that it is possible for attacks to occur when hackers attempt to "spoof" authorized access points in order to "trick" wireless workstations or mobile users into inadvertently connecting to the hacker's access point, thus compromising the wireless network and stealing important information.

3.3.3 Ensuring Privacy

In dealing with security and privacy, the mantra that should be followed is
"A security solution *without* ensuring privacy is *not a solution at all*!!!"
While concentrating on the issues pertinent in wireless security, it is imperative to deal with the issue of privacy. The 802.11 standard can deal with privacy issues through using cryptographic mechanisms in its wireless connectivity.

The WEP mechanism ensures privacy through its use of the RC4 symmetric-key cipher algorithm to create a pseudorandom data sequence. WEP makes it possible for data to be protected from interception (or really understood) between transmission points along the wireless network. WEP is useful for all data in the WLAN, to protect and make the data channel private. The idea is to protect data when flowing through:

- Transmission control protocol/Internet protocol (TCP/IP)
- Internet packet exchange (IPX)
- Hyper text transfer protocol (HTTP)

WEP [4] is designed to permit privacy by supporting cryptographic keys ranging in size from 40 to 104 bits. The idea is that by increasing the size of the key, the level of security

is increased proportionally. For example, a secure setup includes a 104-bit WEP key using 128-bit RC4. In practice, when a key size in excess of 80 bits is employed, it makes brute force hacker attacks very lengthy, time-consuming, and generally unrealistic as a form of breaking into a network without being detected.

In fact, with 80-bit keys, the number of possible keys is so great that even the most powerful computers produced today would not be powerful enough to break the code. Unfortunately, most companies don't use these keys for even the simplest form of protection on their network. Most WLAN implementations use only 40-bit keys. Most hacker attacks are successful on implementations that use 40-bit WEP keys; the majority of WLANs are at serious risk of being compromised.

Keeping Data Intact

One of the advantages of 802.11b is that it ensures that the data transmission remains intact as it follows the wireless path between the wireless workstation and the access point. The idea of this level of security is to reject any message transmission that may have been modified or intentionally altered during its path from point to point.

To maintain privacy, the 802.11 standard [5] was designed specifically to reject any message altered in transit, either by accident or by design. To ensure that data privacy has been maintained, the cyclic redundancy check (CRC) technique is used as a form of encryption. This setup requires that each encrypted packet is "sealed" in a bubble using the RC4 key encryption to scramble the transmission. Only when the packets are received are they decrypted; a CRC check is computed to ensure that it matches the CRC value before it was sent. Should the CRC value not match, then the receiver has a receive error that defines an integrity violation and the packet is thrown away as corrupt.

Managing Keys

One of the problems with the 802.11 standard is that it has no good way of managing keys. The administrators who take care of the wireless network are responsible for several methods of managing keys with respect to:

- Creating keys
- Distributing keys among wireless users
- Archiving/storing keys so that they don't fall into the hands of a hacker
- Auditing who has what cryptographic keys
- Terminating keys that have become compromised

What happens if nobody takes care of these key management issues?

The wireless network is highly vulnerable to a hacker attack. These insecurities include:

- WEP keys are not unique and can be compromised
- Factory default passwords are prominently posted on hacker sites. This means that no matter which access point is using, the network is *vulnerable* if the default administrative password is unchanged since deploying the WLAN.
- Bad keys. Never make a key all zeros or all ones for the sake of convenience. Those types of keys are the first detected by a hacker looking to see how easy it will be to gain access to the wireless network.
- Factory defaults must always be changed as they are the easiest and simplest ways for a hacker to gain access.

The greatest difficulty is that the problem with managing keys grows in proportion with the size of the organization and the number of keys the administrator will need to keep track of the wireless workforce. To indicate how extensive the task of managing keys actually is, consider that it is very difficult to scale the organization to change keys often enough to randomize them sufficiently to protect the network against a hacker attack. In a large environment, the administrator could be dealing with tens of thousands of keys.

In essence, vigilance and time are required, besides the fact that the administrator must know how to protect the WLAN through the effective management of the encryption keys.

3.4 WLAN VULNERABILITIES

There are a number of security vulnerabilities in 802.11 that have unfortunately been discovered by malicious hacker exploits. These vulnerabilities constitute passive types of attacks that are designed to decrypt traffic with respect to algorithms based on statistical analysis and active attacks designed to decipher network traffic. An active attack is basically accomplished by confusing the access point to give up to the attacker information it should not. This is the reason why default passwords and settings should always be changed as soon as WLAN is deployed [12].

The most significant problem rests with WEP, which was itself designed to make a wireless network nearly as secure as the wired Ethernet. The biggest problems result from using the same WEP key over and over again. The more the same keys are used, the greater the chance an attacker will learn this piece of information so that he might ultimately use it against the user for the purpose of accessing the WLAN. The vulnerability here rests in the fact that the same key is used for extended time periods, and nobody really thinks to change it. Therefore, the WEP key, should be changed as often as the logon password.

The *initialization vector* (IV) constitutes the 24-bit field transmitted in clear text as part of WEP. This 24-bit information initializes the RC4 algorithm key string. The IV is basically a short field used for encryption. The IV is meant to protect the information, but a short IV ultimately gets repeated many times over the network when there is a great deal of traffic. The problem is that an attacker may easily use this information to intercept the wireless data channel, find the key stream, and then use this information to decipher the encrypted data on the WLAN.

Since the IV is actually an element from the RC4 encryption key, once the hacker has intercepted this bit of information and can intercept every packet key. Since the RC4 key is weak in and of itself, this could indicate the precursor of a significant attack. In fact, this attack could easily be run a script kiddie because once the secret key is recovered, it is possible to analyze only a small portion of the wireless network traffic and be able to have full access to the WLAN. There isn't any protection for the actual composition of the encryption that WEP has to offer except that the MAC portion of the 802.11 standard uses the CRC element described earlier as a form of privacy protection.

3.5 COMMON SECURITY PITFALLS

Standard can help to find and solve the problems with the WLAN implementation before they become vulnerabilities that hackers can exploit to the organization's disadvantage.

Poor Security, Better than No Security at All!

The most common problem is that the security controls in the wireless equipment are turned off by default out of the box. Although these security features and functions are not all-encompassing to stop hackers, leaving them disabled just puts the network at unjustified risk. Better that the user should have minimal security measures as opposed to having no security enabled.

Short Keys

Most cipher keys are very short; most implementations use only 40-bit encryption keys, which can make the key stream repeat. There is no reason why the user should not at least use larger key sizes when employing encryption techniques. To that end, a key size should be at least 80 bits long. When using longer keys, the likelihood of having them compromised by a hacker is far less. Hackers use "brute force" attacks that basically try

all possible combinations of usernames and passwords to "force" their way into the WLAN. When the hacker's job is made much longer and more difficult, there is a greater likelihood that the intrusion attempt is caught and the network vulnerability is resolved.

Initialization Vectors

Repetition is bad because it makes it easier for hackers to decipher the data channel for the average LAN. Initialization vectors make the cipher stream repeat, and it is that very repetition that creates vulnerability in the WLAN.

Shared Keys

One of the methods meant for protecting the WLAN is the element that can be most easily compromised. "Shared" cipher keys by their very definition constitute a vulnerability because they can be "shared" with hackers as well as legitimate employees. The entire basis of maintaining security is highly dependent on keeping these keys secret and in the possession of authorized users only. Hackers often try every possible username and password combination in order to try and "force" access privileges into the WLAN. The encryption keys must be changed often, otherwise there is very little means to protect the network against a hacker attack.

WEP uses the RC4 keys, but their deployment is poor at best due to the fact that a hacker can sometimes intercept the key just by examining the first few packets. Although this type of interception is often used by more advanced hackers, in fact there a number of automated means that have made this type of attack much more accessible to almost anyone interested in a simple point-and-click interface to run scripts to intercept information pertaining to the wireless network.

Checks and Balances for Packets

It is essential to maintain the privacy and substance of each packet during wireless transmission handled by cyclic redundancy checks. However, CRC is not always

sufficient to maintain the substance of the encrypted packets because it is quite possible for someone to intercept and modify the data channel. This means that these types of protection mechanisms are not sufficient to protect the WLAN from a hacker attack.
Using encryption enables the user to protect himself so that he does not become an easy target for a hacker attack. If the protocols that do not employ encryption are used, the user is leaving himself open to a cryptographic attack on the WLAN.

Authentication

Accessing the network need not necessarily depend on trying to crack the access codes; it could be done by something as simple and easy as stealing the actual wireless network interface card already configured with its unique MAC address to access the wireless network. In the vast majority of WLANs, no authentication is actually taking place. At a minimal level, only verification that the wireless device is set to use the proper SSID occurs. Systems that screen out devices based on identity are highly vulnerable because it is a simple and easy matter to "spoof" or fake the identity of the wireless device based on the SSID.

Sometimes the user only requires just that piece of information to log into the wireless network. How secure is that? Authenticating the device often relies on the simplest form of "shared key challenge response" mechanism. The attack most common in this type of authentication is the hacker who is between the wireless workstation and the access point using challenge response authentication mechanisms that proceed in one direction only. However, an added level of protection is possible when authentication occurs on both sides in order to verify that both the users and network are authorized to use the network resources.

3.6 ATTACK PATTERNS

Wireless attacks are either active or passive, as shown in Figure 3.2.

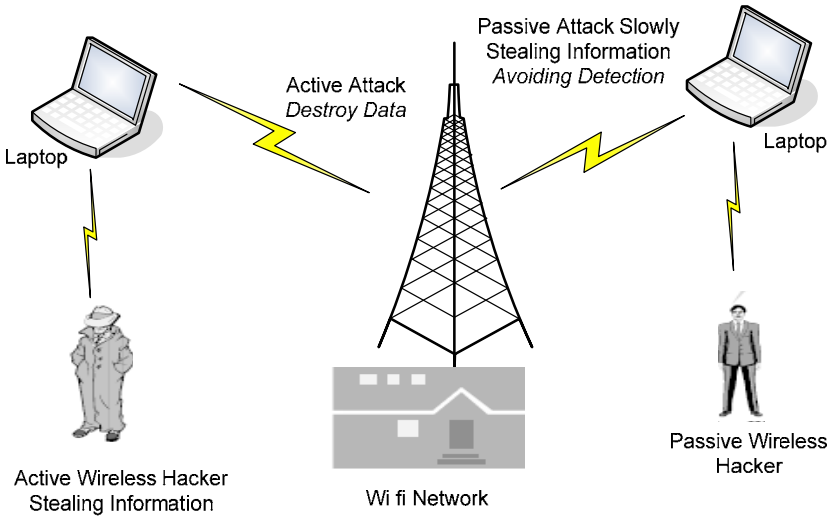

Figure 3.2: Attack Patterns

3.6.1 Active Attack

An active attack constitutes a pattern where a hacker attempts to modify the data channel, messages, or files. With constant vigilance the user will be able to catch this type of attack; however it is difficult to prevent this type of attack without actually pulling the plug of the WLAN. Active attacks include: denial of service (DoS) and message alteration.

Denial of service attacks: A DoS or distributed denial of service (DDoS) is an active attack pattern that prevents legitimate users from using their wireless network. There are a number of risks because these attacks prevent local and remote users from using the network resources. Besides the problems with destroying the network connectivity, the organization also loses business opportunities, revenue, and good public opinion.

Message alteration: In this type of attack, the hacker alters the real message by either adding, erasing, or changing the sequence of the message. This removes the trust factor of the message and makes all the traffic unusable.

3.6.2 Passive Attacks

In these attacks, an unauthorized user acquires access to the network data sources. There is no alteration of message content, but it is possible to eavesdrop on the transmission. Passive attacks are meant not to disrupt, but to acquire information flowing across the wireless network.

Replay: In this type of passive attack, the hacker intercepts or eavesdrops on the data channel. The hacker does not do anything to compromise the systems at first, but can resend altered messages to an authorized user pretending to be the system host.

Eavesdropping: This is a passive attack in which the hacker listens to all the network transmissions in an effort to acquire information flowing from one wireless workstation to the access point.

Traffic analysis: The hacker analyzes the traffic pattern through this type of passive attack to determine what network patterns exist. He can then use all the information acquired to gain information about the traffic from each user on the wireless network.

3.7 WIRELESS SECURITY BEST PRACTICES

This section describes best practices in mitigating the problems described above.

3.7.1 Location of the APs

APs should be topologically located outside the perimeter firewalls. The wireless network segments should be treated with the same suspicion as that for the public Internet. Additionally, it is important to use directional antennae and physically locate them in such a way that the radio-coverage volume is within the control of the corporation or home.

3.7.2 Proper Configuration

There is a large percentage of APs left configured with the defaults. Before a wireless device is connected to the rest of the existing network, proper configuration of the wireless device is necessary. The APs come with a default SSID, such as "Default SSID", "WLAN", "Wireless", "Compaq", "intel", and "linksys". The default passwords for the administrator accounts that configure the AP via a web browser or SNMP are well known for all manufacturers. A proper configuration should change these to difficult to predict values. Unless the default SSID on the AP and stations is changed, SSID broadcasts are disabled, MAC address filtering is enabled, WEP enabled, an attacker can use the wireless LAN resources without even sniffing [9].

The configuration via web browsing (HTTP) is provided by a simplistic web server built into an AP. Often this configuration interface is provided via both wired connections and wireless connections. The web server embedded in a typical AP does not contain secure HTTP, so the password that the administrator submits to the AP can be sniffed. Web based configuration via wireless connections should be disabled.

WEP is disabled in some organization because the throughput is then higher. Enabling WEP encryption makes it necessary for the attacker intending to WEP-crack to have to sniff a large number of frames. The higher the number of bits in the encryption the larger the number of frames that must be collected is. The physical presence in the radio range

of the equipment for long periods increases the odds of his equipment being detected. WEP should be enabled.

The IEEE 802.11 does not describe an automated way of distributing the shared-secret keys. In large installations, the manual distribution of keys every time they are changed is expensive. Nevertheless, the WEP encryption keys should be changed periodically.

3.7.3 Secure Protocols

If the WEP is disabled, or after the WEP is cracked, the attacker can capture all TCP/IP packets by radio-silent sniffing for later analyses. All the wired network attacks are possible. There are real-time tools that analyze and interpret the TCP/IP data as they arrive. All protocols that send passwords and data in the clear must be avoided. This includes the rlogin family, telnet, and POP3. Instead one should use SSH and VPN. In general, when a wireless segment is involved, one should use end-to-end encryption at the application level in addition to enabling WEP.

3.7.4 Wireless IDS

A wireless intrusion detection system (WIDS) is often a self-contained computer system with specialized hardware and software to detect anomalous behavior. The underlying software techniques are the same hacking techniques described above. The special wireless hardware is more capable than the commodity wireless card, including the RF monitor mode, detection of interference, and keeping track of signal-to-noise ratios. It also includes GPS equipment so that rogue clients and APs can be located. A WIDS includes one or more listening devices that collect MAC addresses, SSIDs, features enabled on the stations, transmit speeds, current channel, encryption status, beacon interval, etc. Its computing engine will be powerful enough that it can dissect frames and WEP-decrypt into IP and TCP components. These can be fed into TCP/IP related intrusion detection systems.

Unknown MAC addresses are detected by maintaining a registry of MAC addresses of known stations and APs. Frequently, a WIDS can detect spoofed known MAC addresses because the attacker could not control the firmware of the wireless card to insert the appropriate sequence numbers into the frame.

3.7.5 Wireless Auditing

Periodically, every wireless network should be audited. Several audit firms provide this service for a fee. A security audit begins with a well-established security policy. A policy for wireless networks should include a description of the geographical volume of coverage. The main goal of an audit is to verify that there are no violations of the policy. To this end, the typical auditor employs the tools and techniques of an attacker.

3.7.6 Newer Standards and Protocols

Many improvements in wireless network technology are proposed through proprietary channels (e.g., Cisco Lightweight Extensible Authentication Protocol) as well as through the IEEE. The new IEEE 802.11i (ratified in June 2004) enhances the current 802.11 standard to provide improvements in security. These include Port Based Access Control for authentication, Temporal Key Integrity Protocol for dynamic changing of encryption keys, and Wireless Robust Authentication protocol [13]. An interim solution proposed by vendors is the Wi-Fi Protected Access (WPA), a subset of 802.11i, is only now becoming available in some products .

CHAPTER 4
PROBLEM FORMULATION

As our lives depend more and more on wireless communication, security has become a pivotal concern of service providers, engineers, and protocol designers who have learned that obscurity does not guarantee security and that ad hoc remedies only complicate matters.

Most of the vulnerabilities that exist for wireless medium are the result of medium itself. In particular, because of the broadcasting nature of the wireless networks, the transmissions are freely available to anyone who is present on the network. Wireless LANs are susceptible to the same attacks that plague wired LAN, and also have their own set of unique vulnerabilities. Both wired and wireless networks are subject to the same security risks and issues.

The common vulnerabilities that have been detected in wireless LANs are the ones present due to the mis-configuration of the wireless equipments like access points, deployment of unauthorized equipments, unauthorized access, ad hoc transmissions.

There are other vulnerabilities related to the protocols used. One such protocol is Simple Network Management Protocol (SNMP) which is an application layer protocol that facilitates the exchange of management information between network devices. . Like many network protocols, SNMP has some associated vulnerabilities.

Appropriate management practices are critical to operating and maintaining a secure wireless network. SNMP is the most popular protocol used to manage networked devices remotely. The SNMP protocol enables network and system administrators to remotely monitor and configure devices on the network (devices such as switches and routers).

SNMP uses a community string for authentication purposes. The community string is a password that is used to control access to information residing on a managed device. There are many issues involved with the security of network management through SNMP, which form the bases of this research work.

CHAPTER 5
SNMP VULNERABILITIES IN WIRELESS

Wireless networking has rapidly increased in popularity over the last few years due to the flexibility it provides. The combination of low cost and ease of deployment is leading to rapid adoption of wireless technology. Wireless networks are forcing organizations to completely rethink how to secure the networks and devices to prevent attacks and misuse that expose critical assets and confidential data. While total security of any network is a near impossibility, there are a number of steps to ensure a wireless network will be less likely to be hacked. By their very nature, wireless networks are difficult to roll out, secure and manage, even for the most savvy network administrators.

Simple Network Management Protocol (SNMP) [15] is a request-response protocol that collects management information from network devices and provides a way to set and monitor configuration parameters in a wireless network.This enables the automatic reporting of access point faults to remote IP addresses, together with remote configuration over the network.

Appropriate management practices are critical to operating and maintaining a secure wireless network. SNMP is the most popular protocol used to manage networked devices remotely. The SNMP protocol enables network and system administrators to remotely monitor and configure devices on the network (devices such as switches and routers). SNMP uses a community string for authentication purposes. The community string is a password that is used to control access to information residing on a managed device. Like many network protocols, SNMP has some associated vulnerabilities. There are many issues involved with the security of network management through SNMP.

5.1 OVERVIEW OF SNMP PROTOCOL

The Simple Network Management Protocol (SNMP) is a standard for network management activities [16] defined by the Internet Engineering Task Force (IETF). SNMP is widely used to monitor and manage network devices An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs). A *managed device* is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. An *agent* is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. An *NMS (also called the manager)* executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network. . A simplified SNMP architecture is shown in Figure 5.1

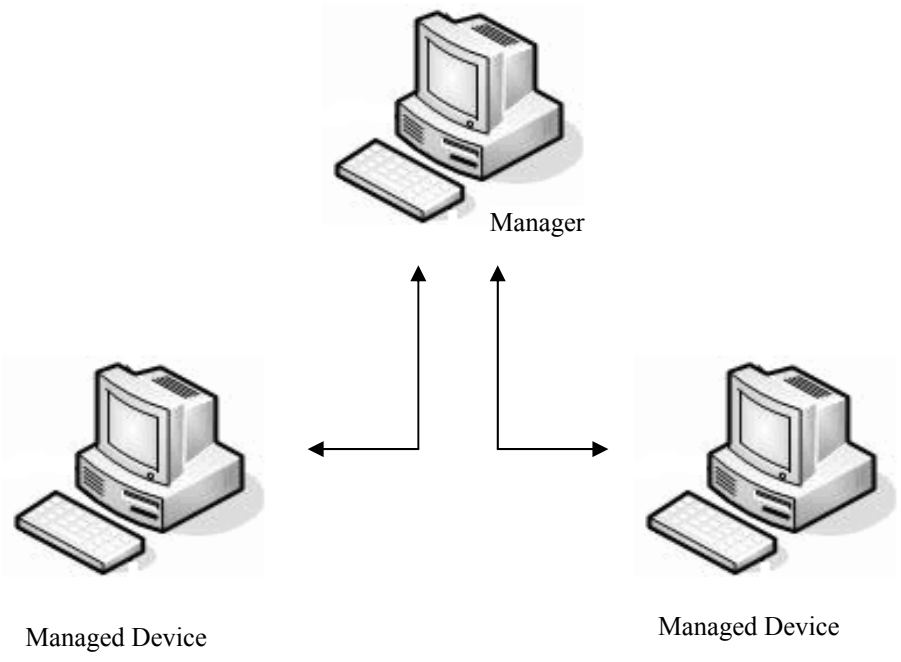

Figure 5.1: SNMP Architecture

The network-management system issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations: *Get, GetNext, Set*, and *Trap*. The *Get* operation is used by the NMS to retrieve the value of one or more object instances from an agent. The *GetNext* operation is used by the NMS to retrieve the value of the next object instance in a table or a list within an agent. The *Set* operation is used by the NMS to set the values of object instances within an agent. The *Trap* operation is used by agents to asynchronously inform the NMS of a significant event

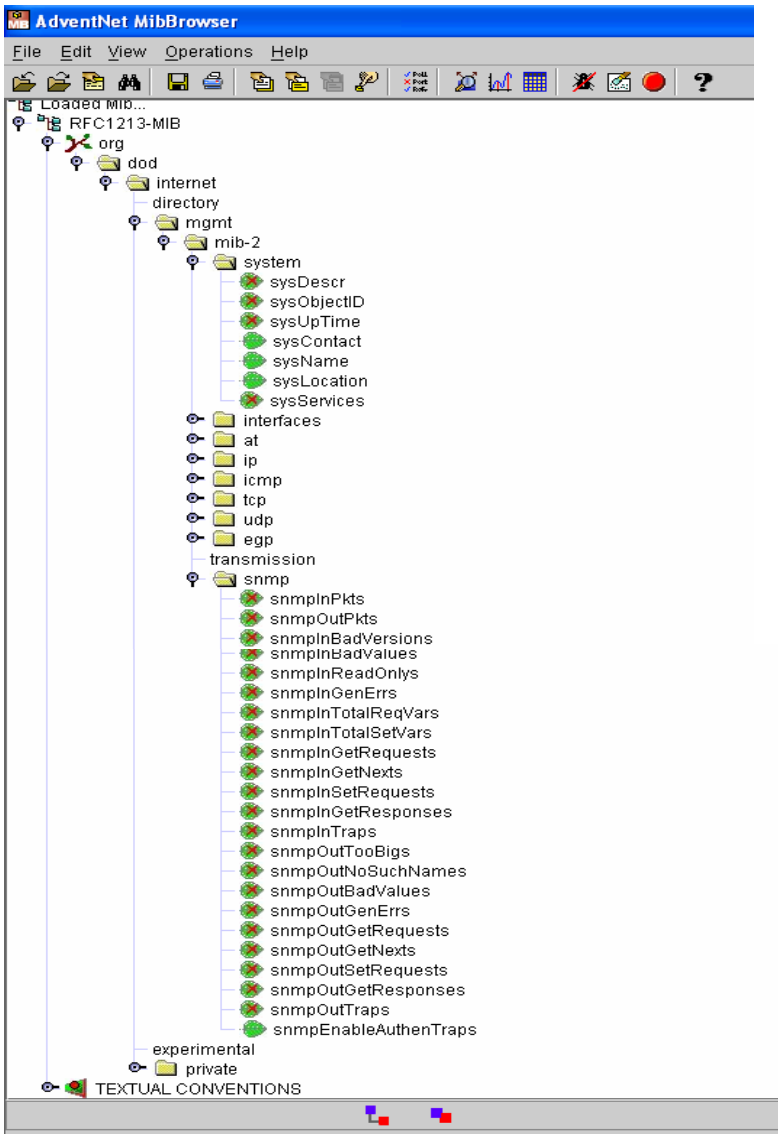

Figure 5.2: MIB structure

A *Management Information Base (MIB)* is a collection of information that is organized hierarchically. MIBs are accessed using a network-management protocol such as SNMP. They are comprised of managed objects and are identified by object identifiers. A managed object (sometimes called a MIB object) is one of any number of specific characteristics of a managed device. Managed objects are comprised of one or more object instances, which are essentially variables. An object identifier (OID) uniquely identifies a managed object in the MIB hierarchy. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. An SNMP binding is a pair formed by an OID and an associated value. SNMP messages contain a sequence of bindings [17].

Figure 5.2 shows the hierarchical structure of MIB 2 using AdventNet MIB browser [18].

5.2 SNMP IN WIRELESS NETWORKS

The Simple Network Management Protocol (SNMP) provides management capability for TCP/IP-based networks and currently is the most widely used standardized network management tool. Therefore, it is natural to adopt SNMP-based management solutions for WLANs. Most of the wireless LAN products offer SNMP to support network management. However managing wireless LANs is a different and harder task as compared to wired network management because of the particular nature of the wireless environment. One of the main problems is the unpredictable behavior of the wireless channel due to fading, jamming, and other environment dependent factors. Signal quality can vary quite dramatically, which might suddenly reduce the efficiency of the management operation.

In wireless networks, SNMP works as follows: SNMP Client is implemented in the Access Point. The external SNMP Manager (running on separate PC over the network) sends requests to SNMP Client which is running on the Wireless Access Point. The request comes from Manager in the form of *Abstract Syntax Notation One (ASN1)* [19]

notation. The SNMP Client parses the request which is in the form of ASN notation and retrieves the data from WLAN driver. After retrieving the data from driver the SNMP Client again encodes the data in the form of ASN notation and sends back the reply message to SNMP Manager.

5.3 USING THE SNMP AGENTS AND MIBS

SNMP network management uses these SNMP agent functions:

- *Accessing an MIB variable:* This function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- *Setting an MIB variable:* This function is also initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value that is requested by the NMS.
- *SNMP trap*: This function is used to notify an NMS that a significant event has occurred at an agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMSs that are specified as the trap receivers under the following conditions:
    - When a port or module goes up or down.
    - When the temperature limitations are exceeded.
    - When there are spanning-tree topology changes.
    - When there are authentication failures.
    - When power supply errors occur.
- *SNMP community strings:* SNMP community strings authenticate access to the MIB objects and function as embedded passwords:
    - Read-only—Gives read access to all objects in the MIB except the community strings but does not allow write access.
    - Read-write—Gives read and write access to all objects in the MIB but does not allow access to the community strings.

- Read-write-all—Gives read and write access to all objects in the MIB including the community strings.

5.4 SNMP VULNERABILITIES IN WIRELESS NETWORKS

Security is an ever-changing topic with new vulnerabilities and more sophisticated attacks coming out on a daily basis. Security Vulnerabilities are a matter of one's unawareness and can be avoided or properly managed as long as we are equipped with good information and a set of best of breed tools.

SNMP based management systems have a number of vulnerabilities and benefits, which have been discussed extensively [20][21][22]. SNMP introduces many vulnerabilities in Wireless Networks.

On the basis of study conducted on the Wi-fi network of Thapar University, the following vulnerabilities are found:

5.4.1 Community string vulnerability

SNMP agents run on many Wireless Access Points. A community defines authentication and access control between an SNMP agent and a management station. The *community name* is used in defining management groups with differing access rights. The community name functions as a password in that management stations must use it for all *Get* and *Set* operations. The same *community name* mapping is used to define access policies for different managers. That is, some names may be restricted to operate only on some of the areas of MIB while the others may have greater rights.

Most of the wireless access points provide an SNMP service with default read−only and read−write community strings of "public" and "private", respectively. These strings, if

not changed by the administrator, will allow remote users to issue an SNMP *GetRequest* or *SetRequest* to the WAP. SNMP can be used to retrieve and modify the device configuration. Also, the potentially sensitive information can be obtained from the access points.

Even if the default community strings are changed by the administrator, they can still be known by sniffing. Tools like Ethereal [23] can be used to sniff the traffic over a wireless networks and get the community strings. Figures 5.3 and 5.4 below show the read-only and read-write community strings of an access point which have been changed to *hidden* and *restrict* respectively.

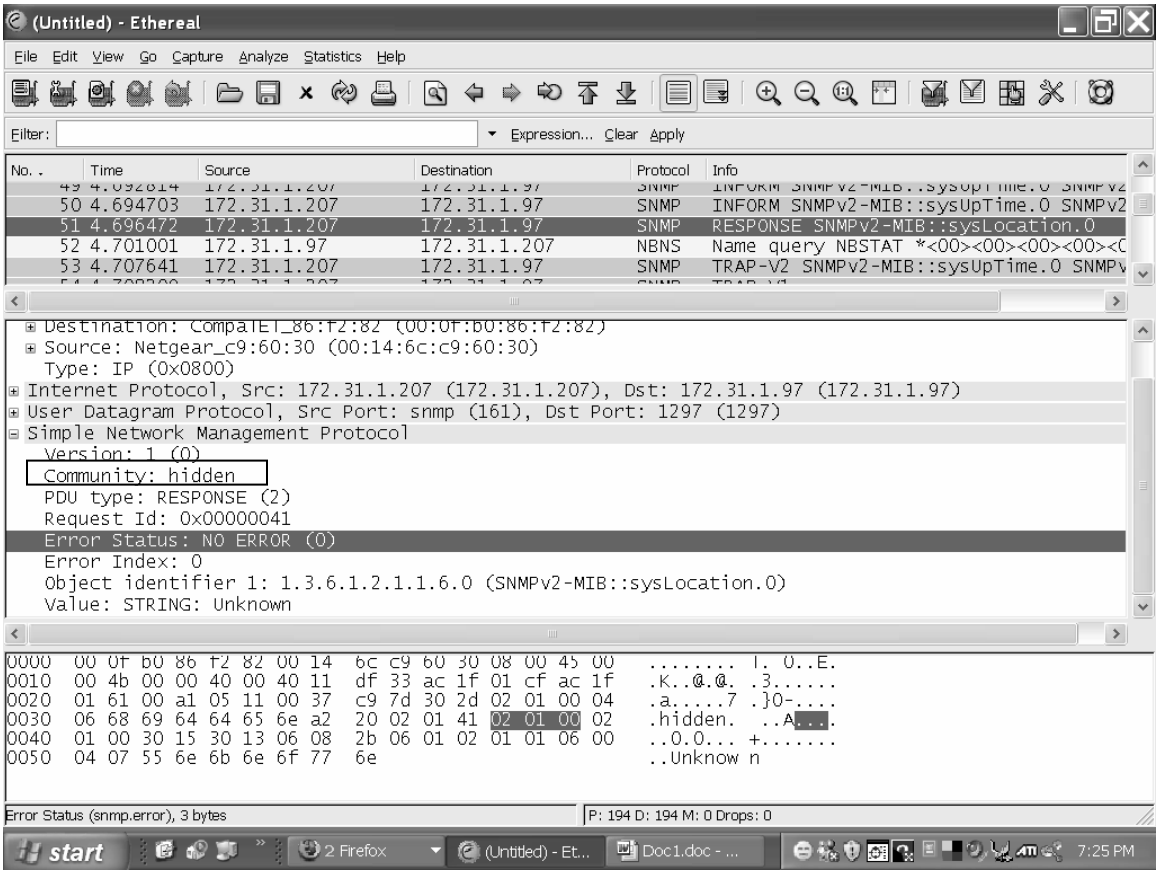

Figure 5.3: Ethereal screen showing the read-only community string of an access point.

The captured packets in the figures indicate that these are SNMP packets with source as Netgear Access point with physical address 00:14:6c:c9:60:30. The read-only

community string (*hidden* in Figure 5.3) and the read-write community string (*restricted* in Figure 5.4), which are transmitted as plain text, are visible in the figure.

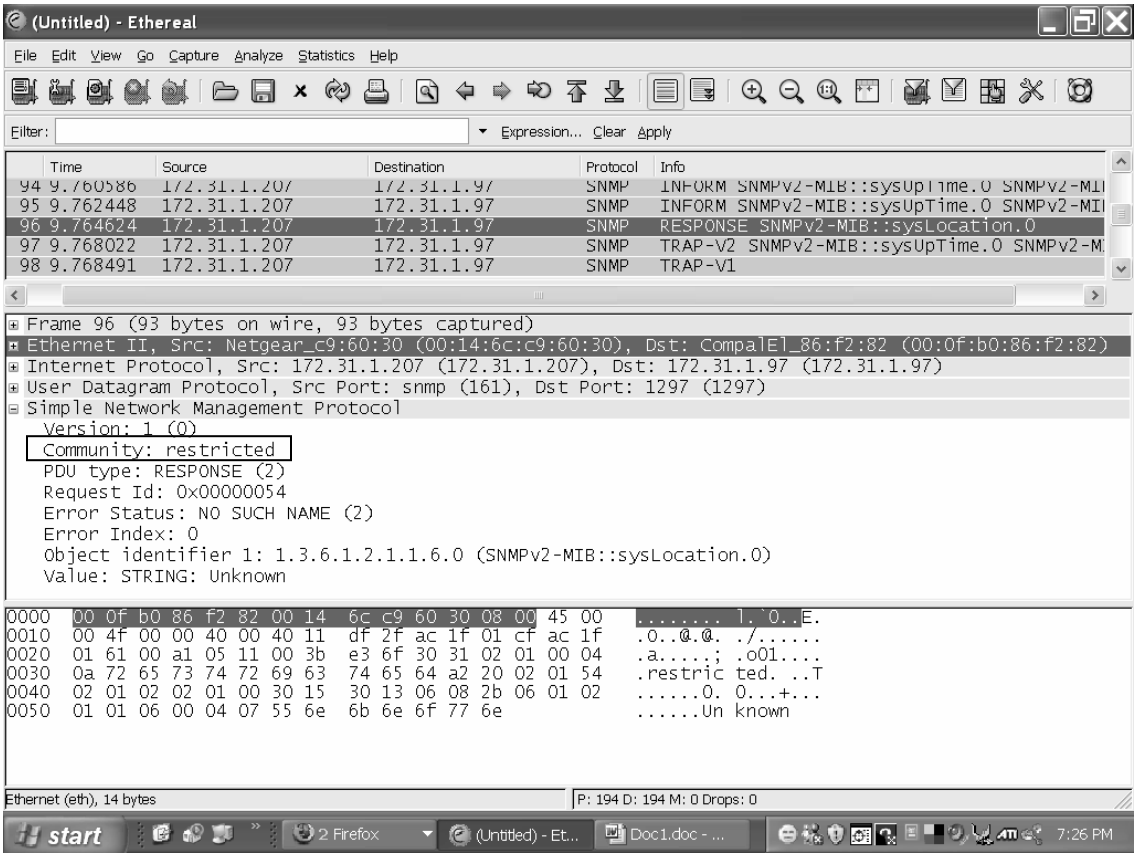

Figure 5.4: Ethereal screen showing the read-write community string of an access point.

5.4.2. One way authentication used in SNMPv3

The one-way authentication used in SNMPv3 leads to the man-in-the-middle (MITM) attack in the wireless network. The MITM can play a dual role: An agent and a manager. In this case, the manager will start managing the agent through the MITM. Moreover, the MITM may take the role of the agent; As a consequence, the manager, which is the non-authoritative entity, will try to synchronize its clock (SNMP engine time, SNMP engine boots) to that of the agent, which is the authoritative entity. This will render all the communication with the authentic device as unauthentic.

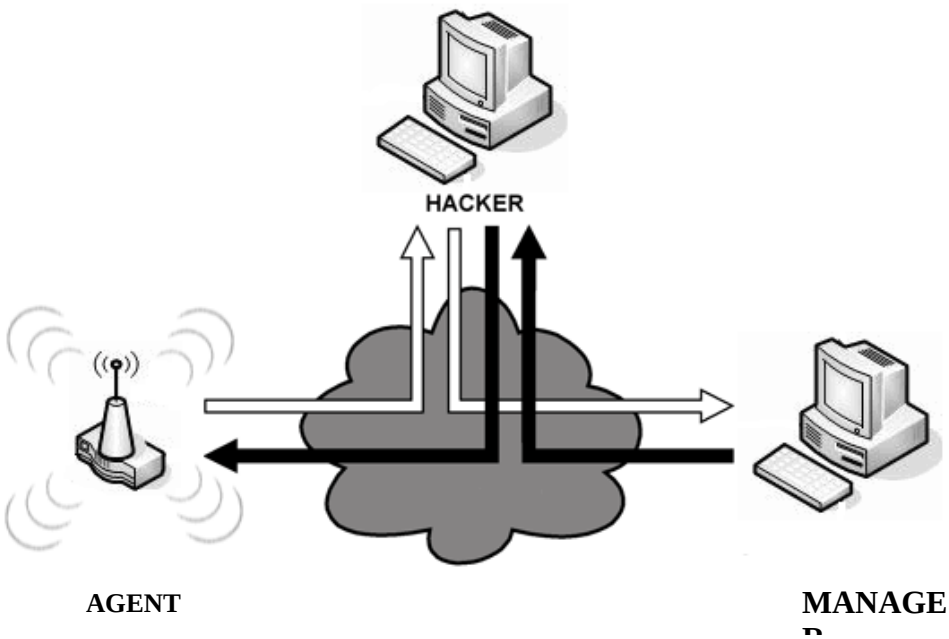

Figure 5.5. Man-In-The-Middle Attack

5.4.3 Hidden SNMP communities

The HP OpenView Management Agent [24] provides a powerful and flexible distributed management solution. This solution is a single interface for centrally monitoring and analyzing multivendor metwork environments.

HP Openview 4.x and 5.x management Agent has a hidden SNMP community string that may allow unauthorized access to certain SNMP variables. Attackers may use this hidden community to learn about network topology as well as to modify MIB variables. ManageEngine Oputils[25] is a tool that can be used to change the MIB variable as given in the figure 5.6.

Figure 5.6:sysName changed using the tool ManageEngine OpUtils

5.4.4 Stopping traps for failed authentication

Traps are enabled by the agents to notify the network management station (manager) of some significant events.SNMP MIB supports an object called *snmpEnableAuthenTraps*, which is used to indicate whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authentication-failure traps may be disabled. It is strongly recommended that this object be stored in non-volatile memory so that it remains constant between re-initializations of the network management system. *snmpEnableAuthenTraps* object can be written within many devices with the help of which an attacker can prevent the device from sending traps for failed authentication. Thus, the attacker can take his time to crack the admin password, without drawing attention to his activity. Once the admin password is discovered, the attacker will be able

to manage all the devices that belong to the manager. In this case, updating the admin password will make no sense since the attacker already knows the old password.

This can be easily done with the help of a network management tool as shown in the Figure 5.7

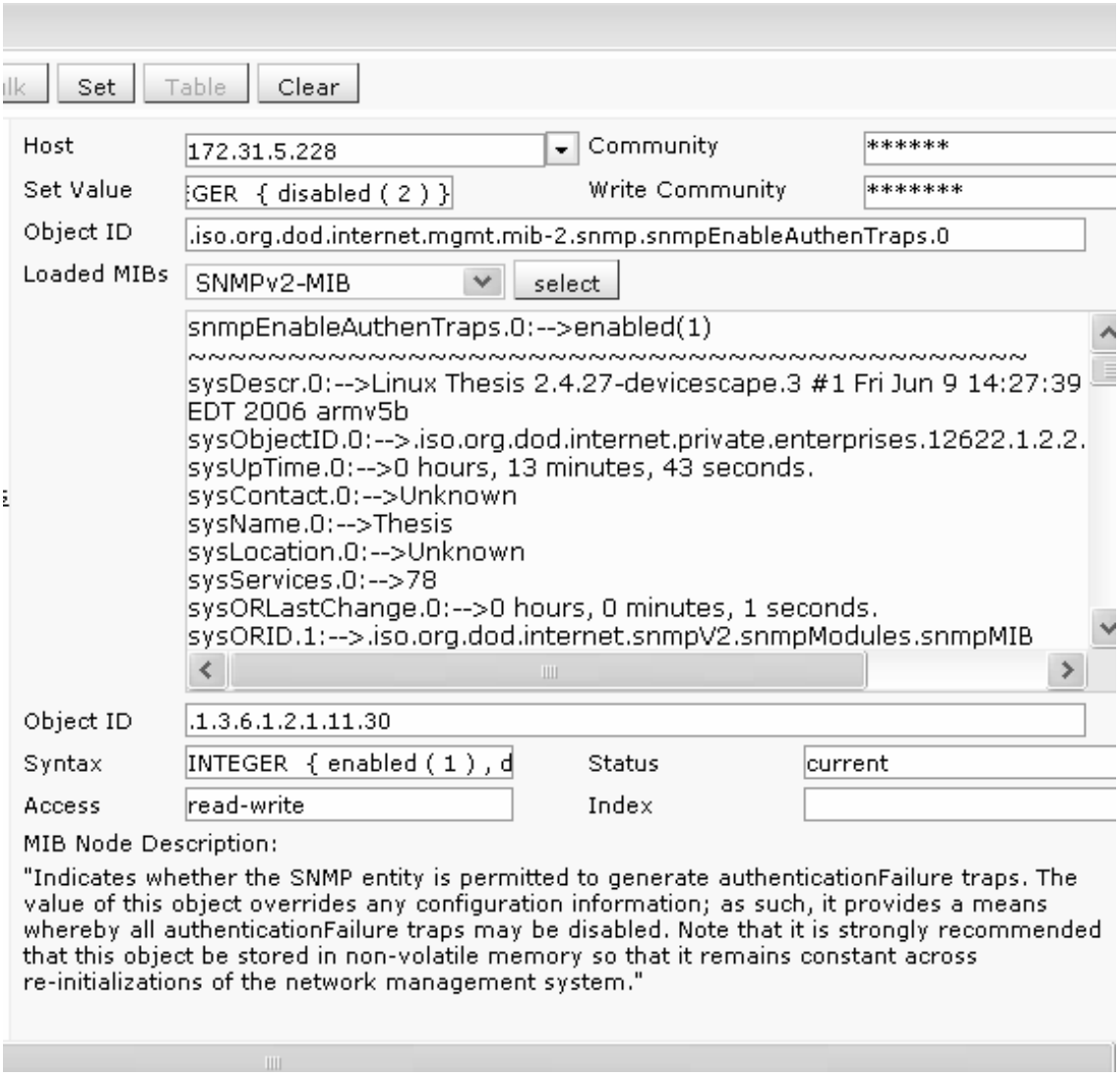

Figure 5.7: snmpEnableAuthenTraps disabled using the tool ManageEngine Oputils

5.5 SUGGESTED COUNTERMEASURES

Following are the few countermeasures that can be used against the above found SNMP vulnerabilities:

5.5.1 Change Default Community Strings

Standardized configurations should be used to reflect the security policy, to ensure change of default values, and to ensure consistency of operation. As already mentioned, most SNMP enabled products have the default community strings “public” for real-only access and “private” for read-write access. These community strings should be changed from the default settings.

Even if the default community string names have been changed, the new community names will still be vulnerable to the packet sniffing. These names are not encrypted; therefore the attacker will have no difficulty in using them to manage the SNMP devices at his will. For greater security, the community strings should be encrypted using a strong encryption algorithm.

5.5.2 SNMP Architecture Modification

The protocol SNMP with its existing security is not sufficient for wireless network, where the intruder has many tools to analyze and crack password. The protocol SNMPv3 (which is the latest and most secure version of SNMP) uses the admin password for one-way authentication and from this password the keys are derived. If an intruder is capable of knowing the password, the intruder can easily manage all the devices in the domain of the manager whose password has been crack. The architecture of the protocol can be improved to include two-way authentication independent of the admin password using the certification authority. The certification authority (CA) is the entity that signs and issues the certificate to both the manager and agent. The Manager and the Agent need to

register and get their public key certificates from CA. So, each of them can easily authenticate the other through this trust model.

5.5.3 Vendor Patches

There should be Configuration/change control and management to ensure that equipment (such as access points) has the latest software release that includes security feature enhancements and patches for discovered vulnerabilities. Most vendors of SNMP-enabled devices have released recommendations for removing the vulnerabilities from their products. The organizations with the wireless networks can check with the vendors of the devices to find out if they have developed patches. Vendor- provided patches improve the handling of malformed SNMP messages in various ways, such as by adding stronger checking to test the validity of incoming SNMP messages.

5.5.4 Restrict Access

Although it is often difficult to block traffic transiting the network, it is possible to identify traffic, which should never be allowed to target the infrastructure devices and block that traffic at the border of the network. Infrastructure Access Control Lists (ACLs) are considered a network security best practice and should be considered as a long−term addition to good network security. This will help in using Authorized Managers list to specify the addresses of the workstations from which SNMP requests are allowed.

5.5.5 Disable the SNMP service

If an organization does not require SNMP service for its wireless network, it is highly recommended to disable or remove this service.

These measures can be used in order to overcome the affect caused by the vulnerabilities of SNMP protocol on the wireless networks.

CHAPTER 6
TESTING

As a case study the wireless network set up at the Thapar University's premises has been studied to carry out the tetsing. Out of various network devices used, Netgear WG302 802.11g [26] wireless access point and D-Link DES 3526 [27] Switches have been used for the study. Following are the specifications of these products.

ACCESS POINT: Netgear 802.11g WG302

Product Description

It supports High-speed networking with IEEE 802.11g, up to 108 Mbps in turbo mode. It has Wi-Fi Protected Access (WPA) security support. It contains Wireless Distribution System (WDS) that supports bridging and repeater modes. Integrated IEEE 802.3af-based Power over Ethernet (PoE) support eliminates extra cables and the need to locate near a power outlet, as the access point is powered over the Ethernet cable. Supports Simple Network Management Protocol (SNMP) MIB I, MIB II, and 802.11 MIB using SNMP-based network management software, such as HP OpenView™. Supports all popular 802.1x port-based authentication protocols, including Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), Protected EAP (PEAP), and Tunneled TLS (TTLS). Console port facilitates local configuration and monitoring. Users can remotely configure, update, and monitor multiple WG302's simultaneously via FTP.

Integrated IEEE 802.3af-based Power over Ethernet (PoE) support eliminates extra cables and the need to locate near a power outlet, as the access point is powered over the Ethernet cable. Supports Simple Network Management Protocol (SNMP) MIB I, MIB II, and 802.11 MIB using SNMP-based network management software, such as HP OpenView™. Supports all popular 802.1x port-based authentication protocols, including Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), Protected

EAP (PEAP), and Tunneled TLS (TTLS). Console port facilitates local configuration and monitoring. Users can remotely configure, update, and monitor multiple WG302's simultaneously via FTP.

Network Management

- Remote configuration and management through Web browser, SNMP or Telnet with command line interface (CLI)
- SNMP management supports SNMP MIB I, MIB II, and 802.11 MIB

Advanced Wireless Features

- Bridging and repeater mode
- Simultaneous wireless bridge and access point mode
- Adjustable transmit power control 100 mW down to 0 mW
- Wi-Fi Multimedia (WMM) to optimize audio, video, and voice applications

Security

- Wi-Fi Protected Access 2 (WPA2) and 802.11i-ready
- Block SSID Broadcast
- VPN pass-through support
- MAC address filtering with access control lists – up to 256 users
- 802.1x RADIUS support with EAP TLS, TTLS, PEAP
- Secure SSH Telnet
- Secure Socket Layer (SSL) remote management login
- Wireless isolation enables peer-to-peer blocking so users may not access another user's PC

SWITCH: D-Link's DES-3526

Product Description:

D-Link's DES-3526 is a high-performance, managed, stackable Layer 2 switch that provides an ideal solution for workgroups and departments. The D-Link Single IP Management (SIM) allows clustering of a virtual stack up to 32 DES-3526 switches with

fewer distance limitation through a single IP address. The clustering environment spans buildings, making it perfect for organization that requires multiple building deployment. The (24) 10/100Mbps Fast Ethernet ports allow desktops to access network resources through flexible 2 Gig uplinks. The entire virtual stack can be managed via a single IP address for simplified network administration.

High-Performance, High Availability L2 Switching

Utilizing an 8.8Gbps switch capacity and support for 8,000 MAC addresses, the DES-3526 Stackable Layer 2 Switch is a wire-speed, high performance switch ideal for workgroups or departments. The DES-3526 supports port trunking with up to 6 trunk groups with 2 to 8 ports in each group per stack. Port trunking enables business users to increase availability and aggregated bandwidth between servers and/or other switches, optimizing the transport of business critical data. The DES-3526 can utilize either the 10/100Mbps or the 1 Gbps port to interconnect up to 32 units within a virtual stack.

Advanced Enterprise Features

The DES-3526 Stackable Layer 2 Switch brings advanced enterprise functions to a more affordable level while supporting advanced features: D-Link Single IP Mangement, L2/L3/L4 (QoS), 802.1x (Port-based Authentication), 802.1x (MAC-based Authentication), and 802.1q (VLANs). L2/L3/L4 (ACLs) can be configured based on: Protocol type, DSCP, MAC Address, IP Address, and/or TCP/UPD Port Number. These features facilitate the deployment of enterprise applications such as: VOIP, streaming media, and multicast content delivery (IP video conferencing and software deployment).

TESTING

The tests were conducted on the network PG Hostel.

Figures 6.1 and 6.2 shows the networks set-up at the PG Hostel

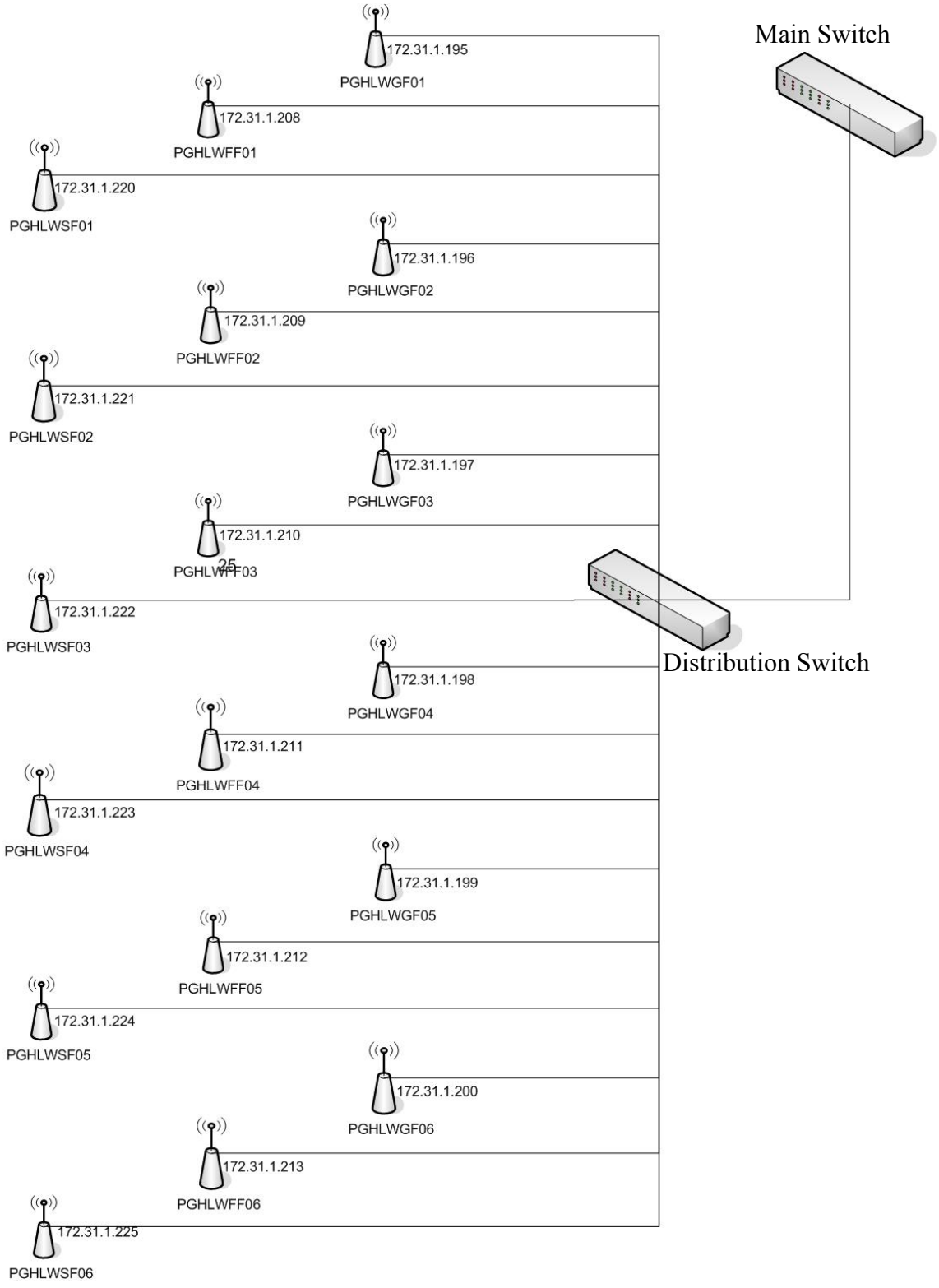

Figure 6.1: Network set-up of the Left-Wing

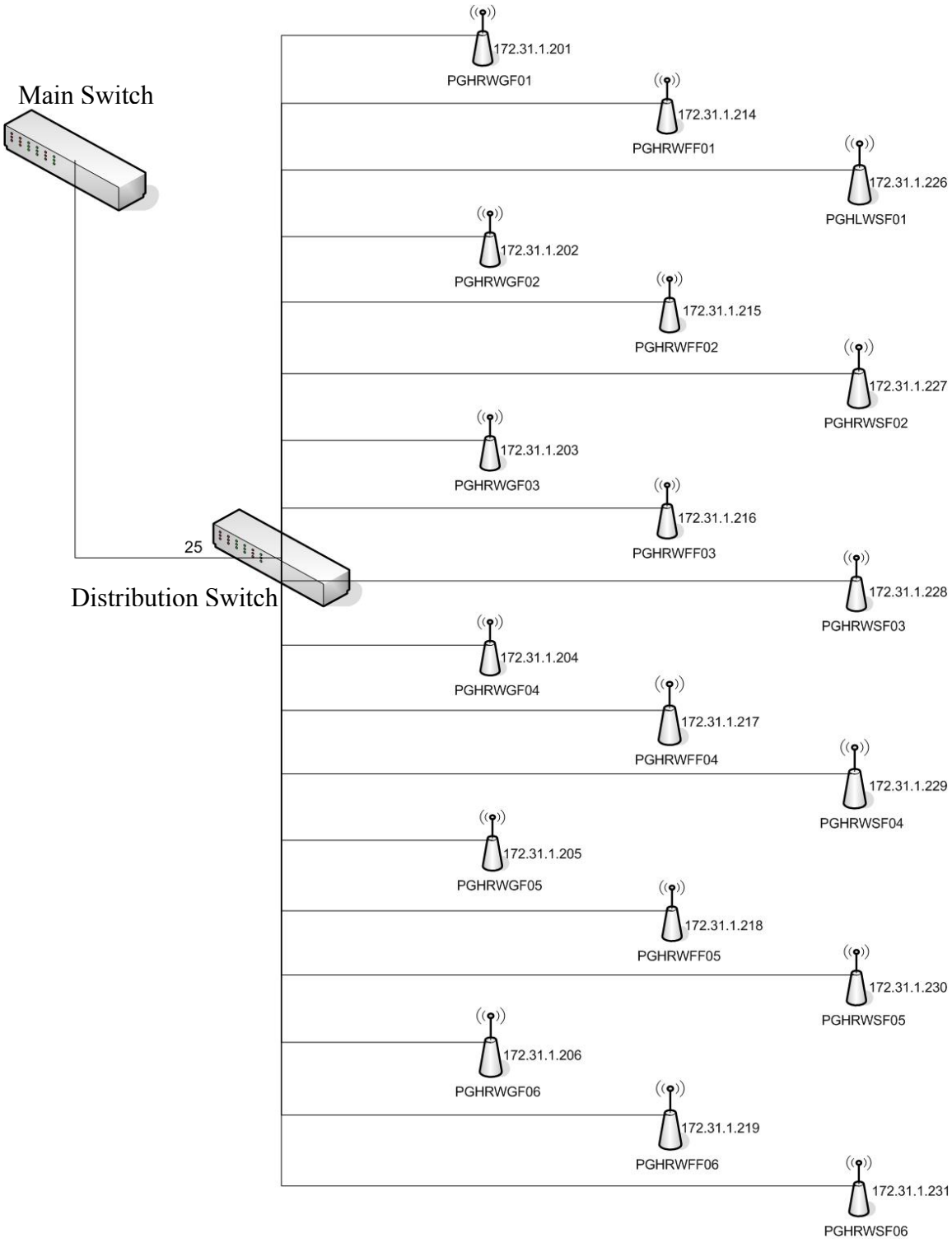

Figure 6.2: Network set-up of the Right Wing

Description:

For establishing the wireless network, PG Hostel is divided into two Wings: Left Wing and Right Wing. Each wing has a Distribution Switch, which is connected to the Main Switch. Each Wing is divided into 18 blocks and each block contains 8 rooms. An access point is provided for each block. Figures contain the Access point names along with their IP addresses.

Following are the tests conducted:

Test Case 1

Test Description: To get the read-only community strings of an SNMP Managed Network device.

Test Environment: Wi-fi

Test Execution: This Test is executed with the help of a network analyzer tool Ethereal. The traffic on the Wi-fi network is captured and analyzed. Figure 6.2 provides the screenshot of the Network Analyzer.

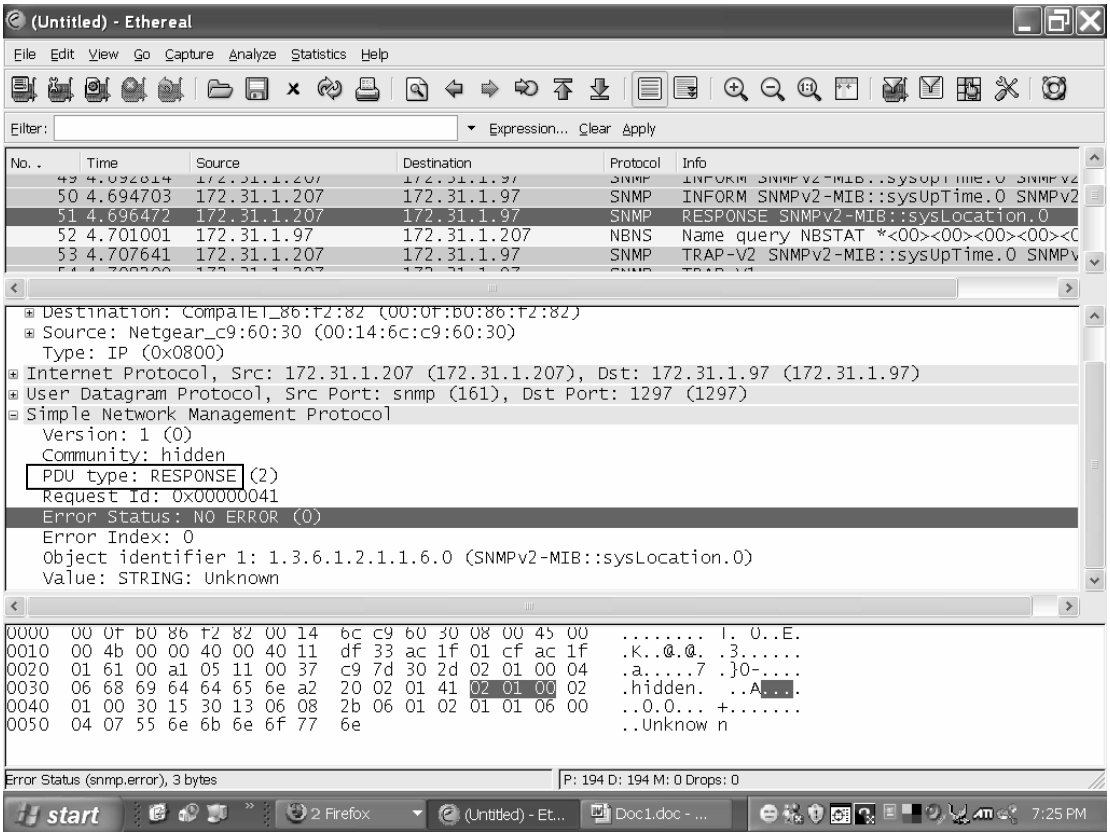

Figure 6.3: Ethereal screen showing the read-only community string

Analysis of the captured data:

Packet Type:	SNMP
Source IP Address:	172.31.1. 207
Destination IP Address:	172.31.1 97
Source MAC Address:	00:0f:b0:86:f2:82
Destination MAC Address:	00:14:6c:c9:60:30
Source Port:	161
Destination Port:	1297
Community:	hidden
Object Identifier:	1.3.6.1.2.1.1.6.0

Result: Read-only community string is found as *hidden.*

Test Case 2

Test Description: To get the read-write community strings of an SNMP Managed Network device.

Test Environment: Wi-fi

Test Execution: This Test is executed with the help of a network analyzer tool Ethereal. The traffic on the Wi-fi network is captured and analyzed. Figure 6.3 provides the screenshot of the Network Analyzer.

Analysis of the captured data:

Packet Type:	SNMP
Source IP Address:	172.31.1. 207
Destination IP Address:	172.31.1 97
Source MAC Address:	00:0f:b0:86:f2:82
Destination MAC Address:	00:14:6c:c9:60:30
Source Port:	161
Destination Port:	1297
Community:	restricted
Object Identifier:	1.3.6.1.2.1.1.6.0

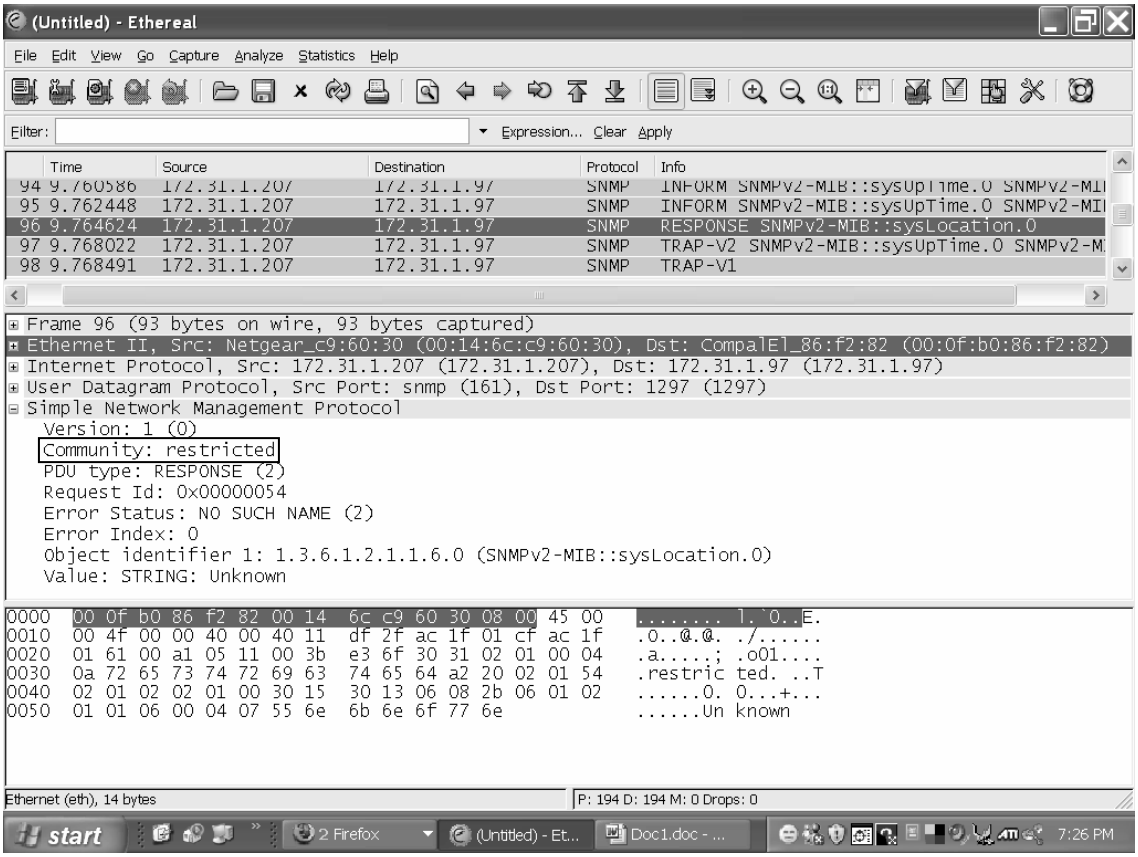

Figure 6.4: Ethereal screen showing the read-only community string

Result: Read-write community string is found as *restricted.*

Test Case 3

Test Description: To check whether MIB variables can be changed or not.

Test Environment: Wi-fi

Test Execution: This Test is executed with the help of a network-monitoring tool ManageEngine OpUtils. An attempt is made to change the MIB variable (sysName) of an access point with IP address 172.31.33.20

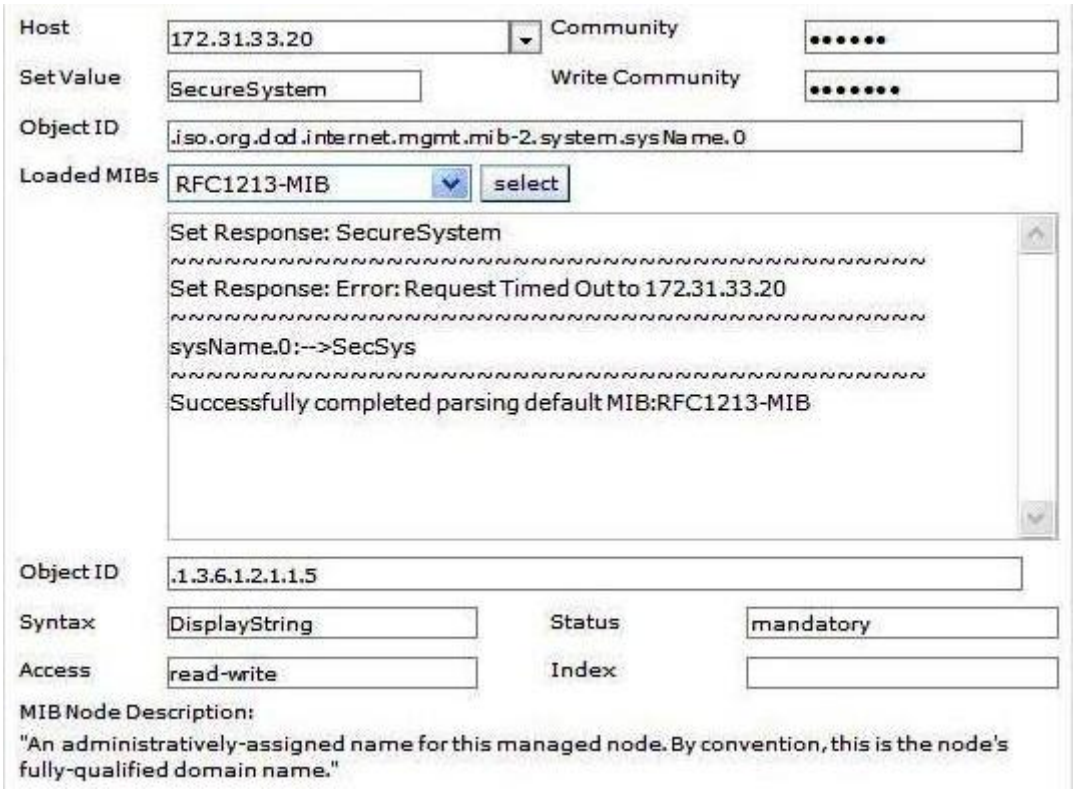

Figure 6.5: MIB variable changed using the tool ManageEngine OpUtils

Analysis of the Output: Value of the MIB variable sysName is changed from *SecSys* to *SecureSystem* by providing the write community and setting the value as *SecureSystem.*

Test Result: MIB variable sysName changed successfully.

Test Case 4

Test Description: To check whether MIB variables *snmpEnableAuthenTraps* can be disabled or not.

Test Environment: Wi-fi

Test Execution: This Test is executed with the help of a network-monitoring tool ManageEngine OpUtils. An attempt is made to disable the MIB variable *snmpEnableAuthenTraps* of an access point with IP address 172.31.5.228

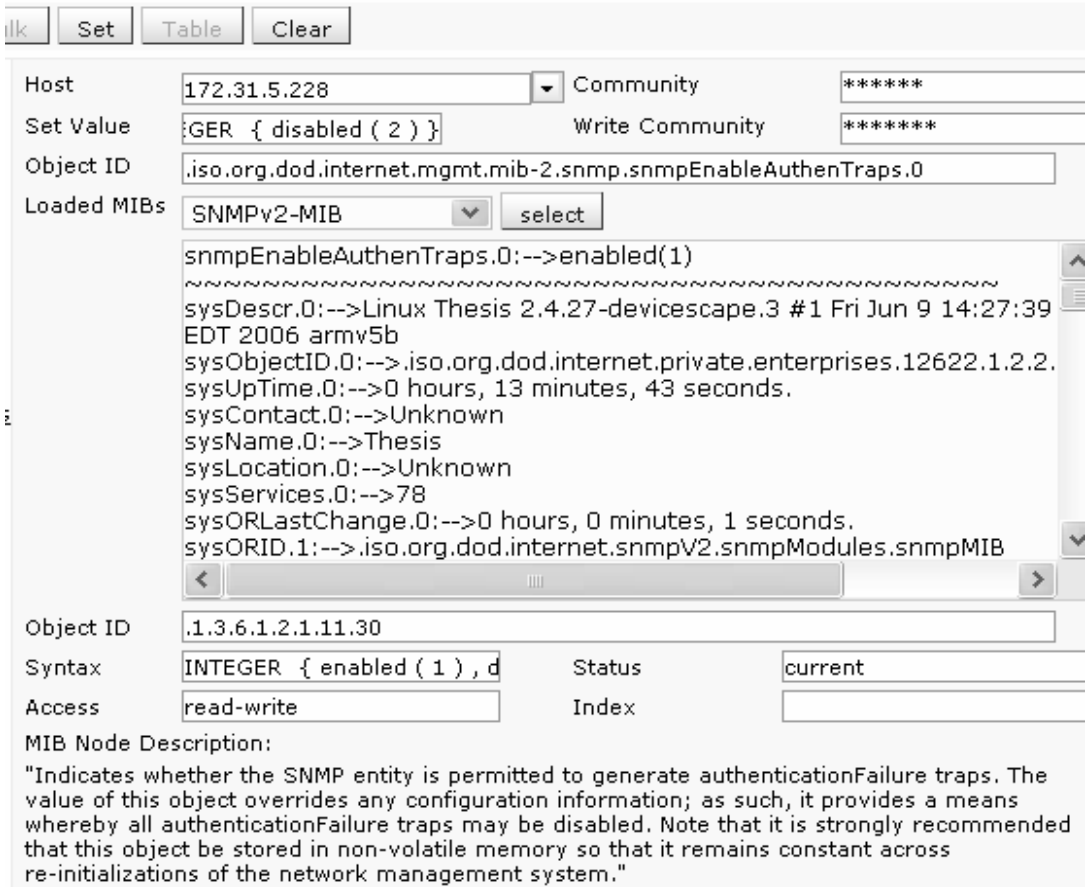

Figure 6.6: snmpEnableAuthenTraps disabled using ManageEngine Oputils

Analysis of the Output: Value of the MIB variable *snmpEnableAuthenTraps* is changed from *enabled* to *disabled* by providing the write community and setting the value as *SecureSystem.*

Test Result: MIB variable *snmpEnableAuthenTraps* changed successfully.

CHAPTER 7
CONCLUSIONS AND FUTURE WORK

7.1 CONCLUSIONS

Wireless security management is a challenging area of increased interest due to the widespread deployment of Wireless LANs (WLANs) and their well-known vulnerabilities to various types of attacks. Until the adoption of the latest security standards is complete, users and network assets on deployed WLANs (802.11a/b/g networks) need to be protected from existing security threats. In addition, while new standards can protect the unauthorized use of network resource for outsiders, they do not deal with the misuse or misbehaviors by insiders.

The challenge is for the network elements to be configured in a correct and scalable manner so that the appropriate global security policies are upheld preventing illegitimate users from gaining access. Lack of security is therefore one of the primary concerns in deploying WLANs for corporate networks in enterprise environments. Wireless networks contain a large number of vulnerabilities that can be exposed. This work explores the security vulnerabilities present in the SNMP enabled wireless network.

Vulnerability detection is a necessity in any system or network because once threats are known, it is more feasible to protect against them. It is possible to manage networks proactively. The countermeasures against these vulnerabilities provided in this work will help in the proactive security of the wireless network. While there are many management products available, network managers should check that their chosen solution provides that managed networks will be secured from any potential attacks. Security of network

management is the key to the security of the entire network and strong security is needed for network management protocols and applications. SNMP is widely used for network management, but it is accompanied by a number of vulnerabilities.

7.2 FUTURE WORK

A wireless network can be penetrated in a number of ways. There are methods ranging from those that demand a high level of technological skill and commitment to methods that are less sophisticated and require minimal technologically skill.

System administrators must continuously scan their systems for security holes and fix the hole on detection. This will tighten the security of system and reduces the chances of security breaches. This process is a continuous process. The security vulnerabilities will keep on arising and process of fixing the security holes will never end.

Future work includes a further study of the vulnerabilities of wireless networks as well as the solutions to the possible security threats. Moreover, further research will explore the latest version of SNMP that in theory provides an improved security protection. Also, the architecture of the SNMP protocol can be modified to make it more secure.

REFERENCES

[1] "Wired Vs Wireless networking" available at http://compnetworking.about.com/cs/homenetworking/a/homewiredless.htm

[2] Jim Geier, "Wireless Networks first-step", Cisco Press, August 03, 2004

[3] Rob Flickenger, "Building Wireless Community Networks", 2nd Edition, O'Reilly.

[4] Matthew Gast, "802.11® Wireless Networks The Definitive Guide**",** O'Reilly, April 2005

[5] "IEEE 802.11 Standard" available at http://standards.ieee.org/getieee802/802.11.html

[6] "Comparison of IEEE LAN Standards" available at http://oit.osu.edu/networking/wireless/Wireless_White_Paper.doc

[7] Barry Lewis and Peter T.Davis, "Wireless Networks For Dummies", Wiley Publishing, Inc., 2004

[8] Stewart S. Miller, "Wi-Fi Security", McGraw-Hill, 2003

[9] "Practical Steps to Secure Your Wireless LAN," a white paper from AirDefense, www.airdefense.com.

[10] "DES Data Encryption Standard" available at en.wikipedia.org/wiki/Data_Encryption_Standard

[11] “AES Advanced encryption Standard” available at http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[12] Wi-Fi Alliance, "Overview—Wi-Fi Protected Access," www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf October 31, 2002

[13] Bernard Aboba and Ashwin Palakar, "IEEE 802.1x and RADIUS Security."

[14] Toby J. Velte, Anthony T. Velte, “Cisco 802.11 Wireless Networking Quick Reference”, Cisco Press, October 20, 2005

[15] “SNMP-Simple Network Management Protocol” available at http://www.snmplink.org/

[16] J. Case, M. Fedor, M. Schoffstall, and J. Davin, “A simple network management protocol (SNMP)” RFC 1157, IETF, 1990.

[17] Matthias Wiesmann, Peter Urban, Xavier Defago, “An SNMP based failure detection service”, 25th IEEE Symposium on Reliable Distributed Systems (SRDS'06)

[18] AdventNet MIB Browser Available at http://www.adventnet.com/products/snmputilities/mib-browser.html

[19] Abstract Syntax Notation One Available at http://asn1.elibel.tm.fr/

[20] W. Stallings, “SNMP, SNMPv2, SNMPv3, and RMON 1 and 2,” Addison Wesley, 1999

[21] B. Pagurek, Y. Wang, and T. White, "Integration of Mobile Agents with SNMP: Why and How," IEEE/IFI Network Operations and Management Symposium, 2000.

[22] Periklis Chatzimisios, Security issues and vulnerabilities of the SNMP protocol, 1st International Conference on Electrical and Electronics Engineering, 2004.

[23] Ethereal: An opensource network sniffer available at http://www.ethereal.com/

[24] HP OpenView Network Services Management solutions available at http://www.openview.hp.com/solutions/

[25] AdventNet ManageEngine OpUtils: A Comprehensive Network Monitoring Toolset available at http://manageengine.adventnet.com/products/oputils/index.html

[26] Netgear Access point WG 302 802.11g available at www.netgear.com/Products/WirelessAccessPoints/WirelessAccessPoints/WG302.aspx

[27] D-Link Switch: DES3526 Available at http://www.dlink.com/products/?pid

[28] "Wi-Fi protected Access (WPA)" available at http://www.tech-faq.com/wpa-wi-fi-protected-access.shtml

[29] Dr. Eric Cole, Dr. Ronald Krutz, Dr. James W. Conley, "Network Security Bible", Wiley Publications Inc, 2005

[30] RC4 Encryption Algorithm available at www.vocal.com/RC4.pdf

LIST OF PAPERS PUBLISHED

[1] Harpreet Kaur Bindra, Maninder Singh, "SNMP Vulnerability in Wireless Networks", in All India Seminar On Cyber Crimes and Security Challenges organized by The Institute of Engineers, Lucknow (April 13-15, 2007)