# Layered Security Approach for Mobile Computing

**Bakare, Mustapha Abiodun**

**(804716)**

**Universiti Utara Malaysia**

**2011**

# Layered Security Approach for Mobile Computing

**A thesis submitted to the College of Arts and Sciences in Partial**

**Fulfillment of the requirement of Master of Science**

**(Information and Communication Technology)**

**Universiti Utara Malaysia**

**February 2011**

**By**

**Bakare, Mustapha Abiodun**

**KOLEJ SASTERA DAN SAINS**
**(College of Arts and Sciences)**
**Universiti Utara Malaysia**

**PERAKUAN KERJA KERTAS PROJEK**
***(Certificate of Project Paper)***

Saya, yang bertandatangan, memperakukan bahawa
*(I, the undersigned, certifies that)*

**BAKARE MUSTAPHA ABIODUN**
**(804716)**

calon untuk Ijazah
*(candidate for the degree of)* **MSc. (Information & Communication Technology)**

telah mengemukakan kertas projek yang bertajuk
*(has presented his/her project of the following title)*

**LAYERED SECURITY APPROACH FOR MOBILE COMPUTING**

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
*(as it appears on the title page and front cover of project)*

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
*(that this project is in acceptable form and content, and that a satisfactory knowledge of the field is covered by the project).*

Nama Penyelia
*(Name of Supervisor)* : **ASSOC PROF. DR.HATIM MOHAMAD TAHIR**

Tandatangan
*(Signature)* : _____ Tarikh (Date) : 8/3/11

Nama Penilai
*(Name of Evaluator)* : **DR. ANGELA EMPHAWAN**

Tandatangan
*(Signature)* : _____ Tarikh (Date) : 8/3/11

# PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master of Science in Information and Communication Technology degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree the permission of copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor or, in their absence by the Academic Dean College of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use of any material from my thesis.

Request for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed:

# ABSTRACT

Mobile technology had been accepted to be a vital and important and advancing application to be made use of in facilitating our way of doing business, because of its mobility nature. This research focus on securing mobile computing devices using layered security approach in order to safeguard wireless network against any possible threat from unauthorized users from coming into the network. Five layered security levels was discussed in the literature review as an effective means of securing any wireless network from cyber terrorists attacks.

The main objective of this research is to deploy Authentication and Access Control security measures under the Network layer security approach, which happens to be one of the steps involved in securing mobile computing devices using layered security approach. The methodology for the research was adopted from SDLC which include Planning, Analysis, Design, Implementation and Evaluation.

Consequently, the findings of the research was hoped to motivate and encourage organizations to incorporate and deploy layered security approach in improving and enhancing their network security against any possible attacks from external mobile users.

## ACKNOWLEDGMENT

I am forever indebted and thankful to the Almighty God for guiding me through the entire length of the way to success and without whose assistance I would never have reach this far and for giving me the strength, wisdom and sound health throughout my period of study in Universiti Utara Malaysia.

I also want to express my warmest and deepest gratitude to my wonderful supervisor in person of Assoc. Prof. Hatim Mohamad Tahir who willingly accepted to supervise, lead and guide me patiently as regard sharing his abundant source of knowledge in this dissertation. I will always be forever thankful and grateful to him because without his beneficial comments, this research would have never been possible.

Once again I thank the Almighty God for His direction and who had made me what I am today. Profound gratitude goes to all the authors whose materials have given me a lot of inspiration in the writing of this project, most of who are referenced.

I am indebted to my beloved parents, Mr. and Mrs. Bakare for all their love and encouragement as well as their financial, moral and spiritual support and for being able to see me through all this years of my studies and for trusting in me.

My appreciation also goes to my siblings in likes of Muyiwa, Wasiu, Kunle and Titilope for their love, assistance and encouragement.

My warmest gratitude also goes to Mr. and Mrs. Ali, Mrs Abudu, Mom Dare, Mom Iqmah, Mr. and Mrs. Odukoya and Mr. Adesiyan for their passionate love shown to enhance my educational development. May God bless you all (Amen).

I also own a lot to my cousins in likes of Lateef, Akeem, Ganiu, Khadijah, Dare, Bose, Damilola, Seun and the rest of the families whose names were not mentioned.

Somebody that you can always count on is your friend. My warmest and strongest appreciation goes to my friends: Mathew, Gbolahan, Sesan, Tola, Bukky, Shola, Folasade, Latifat Afiolaji, Feyi, Ismail, Ayo Omotoso, Ridwan, Okere, Joe, Jelal, Mr. Aliyu, Mohammad Ali, Tunde Adelaja, Ayo Adelaja, Jide Adelaja, Ifalaju, Kelechi, Segun Adebambo, Oyuke, Onuoha, Olamide, Sunday Sejoro, Jide Kuye, Abayo, Remi, Yemi Aleje, David Oduyebo, and so many others whose names were not mentioned. Am using this privilege to say a big thank you for being a friend indeed may the Almighty God continue to strengthen the cord of love that binds us all together. I love and appreciate you all.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER ONE

# BACKGROUND OF THE STUDY

## 1 Introduction

Today wireless networks have gained increasing popularity, providing users with both mobility and flexibility in accessing information. However, existing trends have shown that wireless LAN networks have been exposed to security vulnerabilities, such as risk, threats and attacks (Baghaei, & Hunt, 2004).

To mitigate these risks, agencies need to adopt security measures and practices that help bring their risks to a manageable level (Karygiannis & Owens, 2002). There is a need for a well secured wireless network system, despite its numerous advantages such as strong return on investment, lower installation cost, higher availability and mobile connectivity. The risks to users of wireless mobile computing technology have increased exponentially as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the working place.

Karygiannis & Owens, (2002) founded that there are various numbers of security risks associated with wireless technology. At corporate level, it is the responsibility of the IT department to keep up to date with the types of threats including appropriate counter measures to deploy. Security threats are growing in the wireless area. Crackers have learned that there is much vulnerability in the

current wireless protocols, encryption method, and in the carelessness and ignorance that exists at the user and corporate IT level. Method of cracking has become much more sophisticated and innovative with wireless cracking has become much more accessible with easy-to-use window-based tools being made available on the web at no charge.

Layered security strategy addresses each layer of a network configuration by deploying a leverage security solution, such as allowing each of the layers to be designed in modules in order to protect organizations from many security challenges that exist today (Kurose and Ross 2008).

Different layers can be assigned to different standards, committees, and design terms; it is also possible to plug in different machines at different layers. It increases the compatibility of different machine. Ultimately, a solid approach to network security not only ensures security of your network, but all network reliability, business continuity and business production. Securing the network by prohibiting unauthorized access from within can prove to be a daunting challenge.

Nowadays, business must guarantee uninterrupted access to network resources and the application they support; such as IP telephony including unified communications services. Mobile computing encompasses a number of technologies and devices, such as wireless Laws, notebook computers, etc. Basically, any electronic devices that help you unify your life, communicate with coworkers or friends, or do your job more efficiently is part of mobile computing.

## 1.1 Problem statement

Presently, many security approaches within the province of unlayered security for instance, Wired Equivalent Privacy (WEP) used in securing mobile computing devices tends to be globally popular in the security realm. However, they have been discovered to have security gaps due to their lack of guaranteeing full security provisions (Tillwick, & Oliver, 2004). Consequence to the above, this study therefore will address the following research questions.

## 1.2 Research Questions

1. What are the possible weaknesses attributable to securing mobile computing devices using unlevered security approach?

2. What are the steps involved in securing mobile computing devices using layered security approach?

3. What are the measures to be taken in formulating a layered security approach?

## 1.3 Research Objectives

The main objective of this study is to deploy Authentication and Access Control security measures under the Network layer security approach, which happens to be one of the steps involved in securing mobile computing devices using layered security approach. Specifically the study seeks to achieve the following objectives.

1. To identify the possible weaknesses for securing mobile computing device using unlayered security approach.

2. To uncover the steps involved in securing mobile computing devices using layered security approach.

3. To formulate a layered security approach for mobile computing devices.

## 1.4 Scope of the Study

This research is limited to the Network Layered security approach that will only emphasize on Access Control (Authorization) and Authentication.

## 1.5 Significance of the study

The findings of this study will assist organizations to realize the importance of using layered security architecture in securing their mobile computing devices which invariably will lead to a better achievement of their overall performance.

## 1.6 Limitation of the study

Although the overall layered security approach is in total of five but considering the time duration the research work will be limited to only one layered security approach (Network).

## 1.7 Summary

This chapter discussed a general background of the study, as well as the research problem that needed to be solved. The objectives were formulated based on the research question, the scope of the study was briefly mentioned, and of what significance does the study has concerning business organization.

# CHAPTER TWO

# LITERATURE REVIEW

## 2 Introduction

In the previous Chapter, the background and brief description of the research project settings and framework were introduced, and as such, in this Chapter, related or earlier studies concerning mobile technology as well as layered and unlayered security architecture for securing mobile technologies will be put into consideration.

## 2.1 Mobile Technology

A mobile computing device is a laptop or PDA, or any other device that does comparable functions, sideways with storage media and peripherals connected to the device. Mobile computing systems are computing systems that may be easily moved physically and whose computing capabilities may be used while they are being moved. Examples are; laptops, personal digital assistants (PDA's) and mobile phones. By distinguishing mobile computing systems from other computing systems; there will be need to identify the distinctions in the tasks that they are designed to perform, the way that they are designed, and the way in which they are operated. There are many things that a mobile computing system can do that a stationary computing system cannot do; these added functionalities are the reason for separately characterizing mobile computing systems. Among the distinguishing aspects of mobile computing systems are their prevalent wireless network connectivity, there small size, the mobile nature of their use, their power sources, and their functionalities that are particularly suited to the mobile user. Because of these features, mobile

computing applications are inherently different than application written for usage on stationary computing systems.

According to Turisco and Case (2001) recent items in the press indicating the widespread adoption of wireless include:

- The number of wireless Internet users will reach 83 million by the end of 2005, or 39% of total Internet users.

- By the end of 2004 there will be 95 million browser-enabled cellular phones and more than 13 million Web-enabled personal digital assistants (PDA).

- The wireless LAN market is expected to reach $1 billion in 2001; this figure will double by 2004.

In fact, these items refer to different technologies. The first refers to the wireless Internet; the second is about Internet ready devices, and the last refers to wireless LAN. Probably the most common misconception is that wireless means the Internet. Actually, wireless refers to the underlying technology that supports the transport of data between the mobile devices and the main computer system without a wired connection between them. The Internet is a global network that provides access to information and applications using a browser or Web navigation application. Among some of the mobile computing devices and their comparisons can be depicted in figure 2.1 and Table 2.1 respectively.

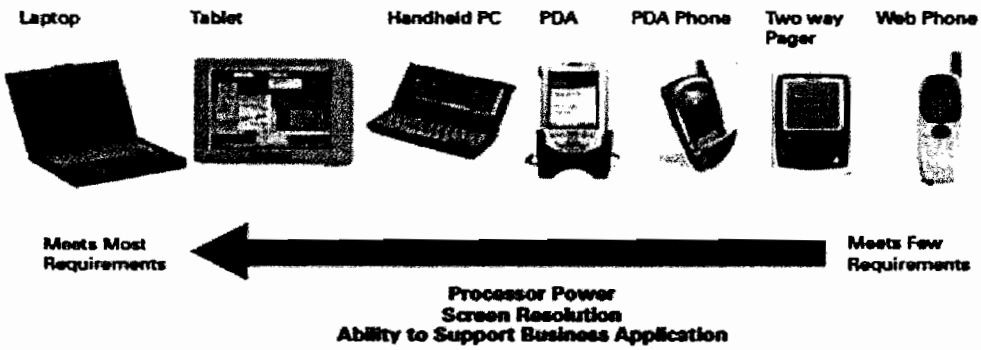



**Figure 2.1: Mobile Computing Device (Turisco, & Case, 2001)**

**Table 2.1: Comparisons of Mobile Computing (Turisco, & Case, 2001).**

| Device Type | Product Features |
|---|---|

To unravel these misconceptions and understand what mobile computing can offer, it is important to recognize that mobile computing is not one technology. It is a range of solutions that enable user mobility by providing access to data anytime, from any location. For

businesses a high level understanding of wireless technology and mobile computing options is fundamental to sound decision-making on whether and in what ways to use them.

According to koudonnas and Iqbal (1996) mobile technology is that technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link. Mobile computing represented the inevitable direction of network development, which made it true that people use computer resources according to their wills (Jeong, & Baik, 2002). Depicted below is the wireless landscape diagram (Figure 2.2)

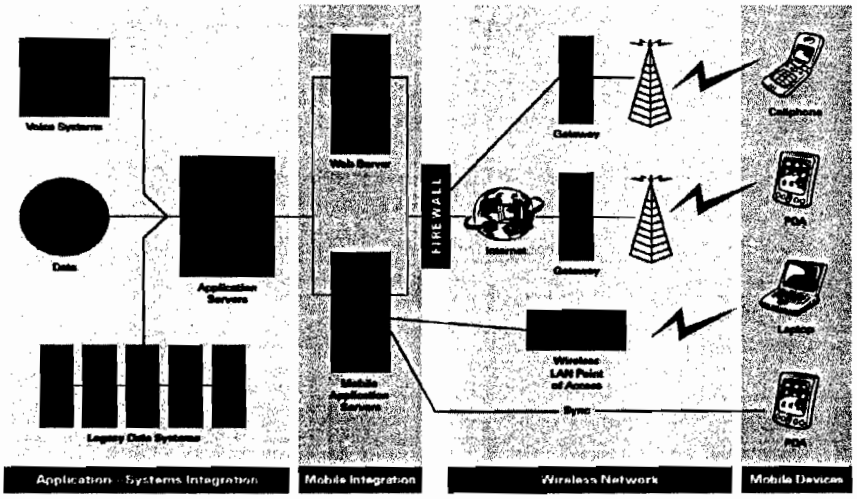



**Figure 2.2: Wireless Landscape Diagram (Turisco, & Case, 2001)**

Nevertheless, today most people are equipped with mobile devices and most of them already have good knowledge and experiences in using mobile devices to access internet applications (Dankers, Garefalakis, Schaffelhofer, & Wright, 2002). As shown in figure 2.3 are some of the mobile computing infrastructures (Turban, Leidner, Mclean, & Wetherbe, 2007).

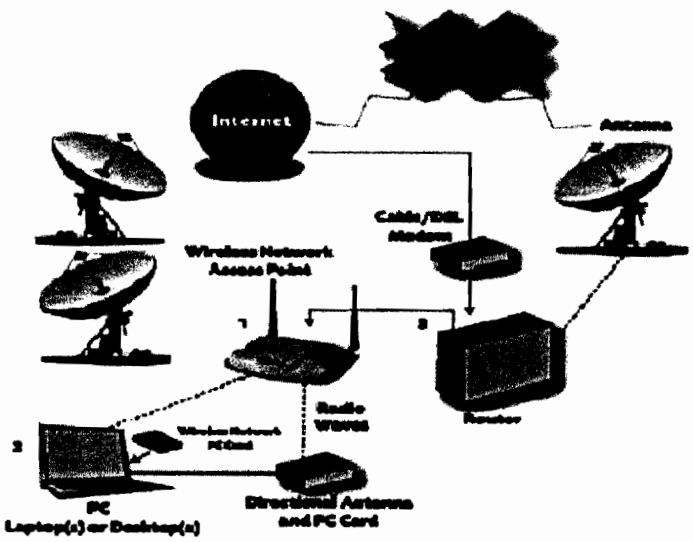



**Figure 2.3: Mobile Computing Infrastructure (Turban, Leidner, Mclean, & Wetherbe, 2007)**

According to Schei and Fritzner (2002) the number of subscribers of mobile devices such as mobile phones has also increased in the same period in Norway. Even though, the number of subscribers was already substantial, it grew approximately 30 percent. In 2001, 3,201,554 individuals were mobile phone subscribers. That is 71% of the population, with comparison, only approximately 30% of the population in the USA has mobile subscription. Consequently, based on Chenand Kinshuk (2005) China has 206 million subscribers in 2002, which is 16.19% of China's population.

Notwithstanding the exponential progress of CPU speed, modern computers cannot survive with the growing demand for computational resources that occur in areas such as bio-informatics (Wang, Liu, Wang, & Chen, 2004). According to Hu and Meng (2005) the characteristic of mobile computing environment is the ceaseless changing of resources, and changes in a limitation. So in the environment with restrictive resource, the usable resources should be correctly used, and when the quality of usable resources drops or the usable resources become to be unusable, the system should be fit for the changes. Moreover,

mobile computing users may be transfer from one network to another in the mobile process, which means to support the operation of network transferring.

A study conducted by Turisco and Case (2001) explained that mobile computing is becoming an important part of health care's information technology (IT) toolbox. Technology advances and the proliferating health care applications indicate that mobile computing will find a secure place in both inpatient and outpatient care. It is not too early for organizations to investigate the benefits it can offer and how it would fit in with current information systems, workflow, and care practices.

According to him, he stated that mobile computing is not a single technology, but a combination of three components, that has to do with handheld computing device, connecting technology, and a centralized information system, each with different performance considerations, costs, and risks. To implement mobile computing devices successfully, it will require employing all of these components in the way that best suits the work and environment of the end users. Of recent the popular press and trade had fully ascertained cover stories surrounding mobile computing and wireless technology as the linkage solution for personal communication and business transactions (Turisco, & Case, 2001).

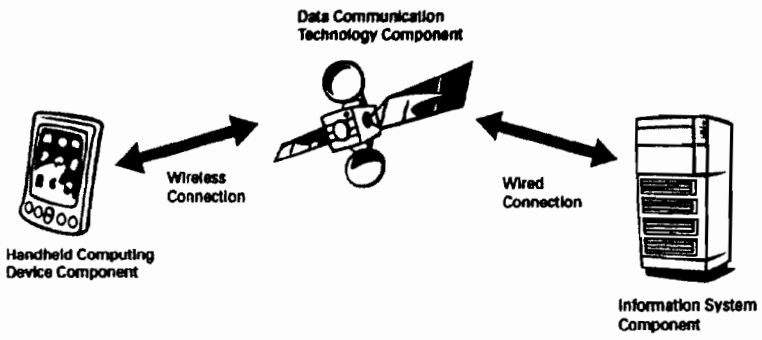



**Figure 2.4 : Mobile Computing Component (Turisco, & Case, 2001).**

As shown in figure 2.4 above mobile computing has three components:

1. Handheld, mobile computing device,
2. Connecting technology that allows information to pass back and forth between the site's centralized information system and the handheld device, and
3. Centralized information system.

The processes involve in the mobile computing devices is similar to the way worker's desktop PC accesses the organization's applications, except that the users device is not physically connected to the organization's systems. The communication between the user's device and the site's information systems uses different methods for transferring and synchronizing data, some involving the use of radio frequency (RF) technology (Turisco, & Case, 2001).

As shown in Figure 2.5 Wireless Local Area Networks (WLANs) offer a quick and effective extension of wired Local Area Networks (Wired LAN) by simply installing access points to the wired network, personal computers and laptops equipped with wireless LAN cards can connect with the wired network at broadband speeds (or greater) from up to 300 yards away from the wireless access point. This means computers are no long tied to the infrastructure of wires.

The majority of WLAN deployments have used a wireless transmission standard known as 802.11 The IEEE 802.11 b standard operates at the radio frequency or 2.4 GHz .a frequency that is unregulated by governments. The 802.11 b standard offers connectivity speeds of up to 11 Mbps, which provides enough speed to handle large e-mail attachments and run bandwidth-intensive applications like video conferencing. While the 802.11 b standard now dominates the wireless LAN market, other variations of the 802.11 standard are being

developed, or have already been approved, to handle increased speeds.802.11g is the latest standard variation, which offers wireless speeds of up to 56 Mbp.

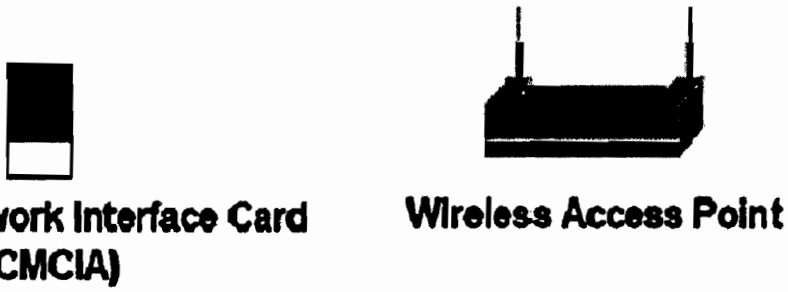



**Figure 2.5: Basic WLAN Components (Burrell, 2002).**

### 2.1.1 Wireless Data Transfer Options

The three most commonly used wireless data transfer methods in today's market are:

1. Wireless Local Area Networks (Wireless LAN)

2. Wireless Internet or Wireless Web, and

3. Data Syncing "hot syncing". This is not a wireless data transfer method, although it is often referenced as "wireless". Data syncing uses docking cradles or docking stations that are connected to a LAN to transfer data from the device to the organization's information system.

### 2.1.2 Wireless LAN

According to Turisco and Case (2001) Wireless LAN is a flexible data and communications system used in addition to, or instead of a wired LAN. Using radio frequency technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections and enabling user mobility. Unlike some technologies such as infrared, wireless LAN is not a "line-of-sight" technology. Therefore the handheld device can operate anywhere within the coverage area. As shown in figure 2.6 as below is the WLAN diagram (Turisco, & Case, 2001).

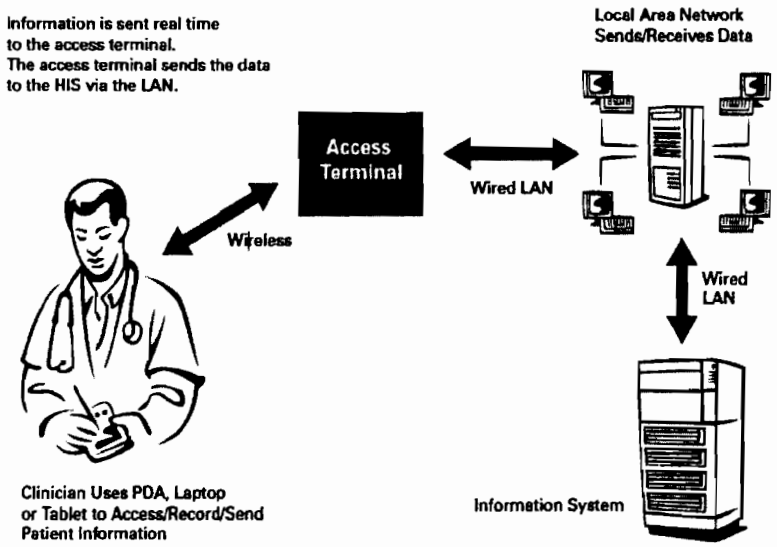



**Figure 2.6: Wireless LAN Diagram (Turisco, & Case, 2001)**

### 2.1.3 Benefits of Wireless LAN

Some of the benefits of deploying wireless LANs can be summarized below:

(I) **Attractive price:** Deploying a wireless LAN can be cheaper than a wired LAN because you do not have the need for wires; simply hook up an access point and it can provide service to multiple computers.

(II) **Mobility:** Boost user productivity with the convenience of allowing them to wirelessly connect to the network from any point within the range of an access

point.

(III) **Rapid and flexible deployment:** Quickly extend wired networks with the ease of attaching an access point to a high-speed network connection.

(IV) **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.

(V) **Performance:** WLANs offer a high-speed connection that, while equal to Ethernet, is quickly passing it in speed.

### 2.1.4 Wireless Internet

Wireless Internet also known as Wireless Web, provides mobile computing access to data using the Internet and specially equipped handheld devices which can be depicted in Figure 2.7 as shown below:

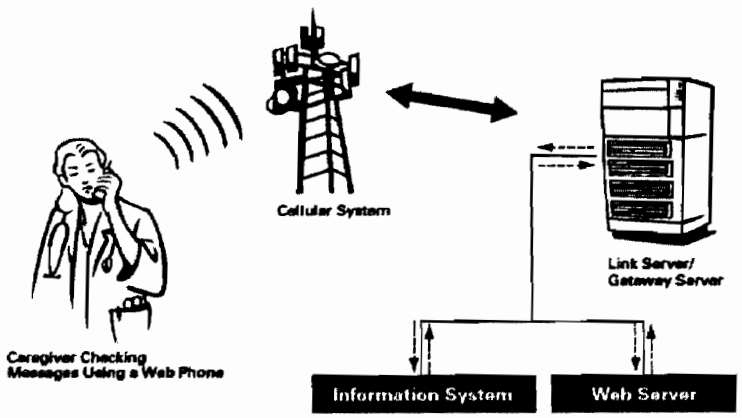



**Figure 2.7: Wireless Internet Diagram (Turisco, & Case, 2001)**

### 2.1.5 Data Synchronization

Data Synchronization as shown in Figure 2.8 ("data syncing") provides many of the benefits of mobile computing without the cost of installing wireless LAN equipment or needing access to the Internet. Information is periodically downloaded from organizations information system to the handheld device and then uploaded from the device to the organization information system. Data syncing is not a wireless data transfer method because data are transferred from the mobile computing device to the organization's information system through a docking (or syncing) cradle wired to the LAN. It is commonly grouped under the general term of wireless, because the user's device is physically attached to the LAN only during the batch data transfer.

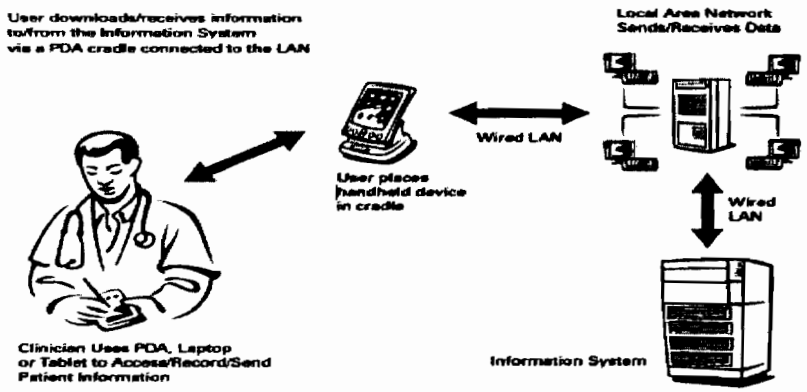



**Figure 2.8: Data Synchronization Diagram (Turisco, & Case, 2001)**

## 2.2 Mobile Application

According to Koudonnas and Iqbal (1996) certain questions always arise concerning the issue of purchasing a mobile computer by businesses, such as "Will it worth it?" In many fields of work, the ability to keep on the move is vital in order to utilize time efficiently. Efficient utilization of resources that is staff can mean substantial savings in transportation costs and other non-quantifiable costs such as increased customer attention, impact of onsite

maintenance and improved intercommunication within the business. The importance of Mobile Computers has been highlighted in many fields of which a few are described below:

(I) **Estate Agents:** Estate agents can work either at home or out in the field. With mobile computers they can be more productive. They can obtain current real estate information by accessing multiple listing services, which they can do from home office or car when out with clients. They can provide clients with immediate feedback regarding specific homes or neighborhoods, and with faster loan approvals, since Applications can be submitted on the spot. Therefore, mobile computers allow them to devote more time to clients.

(II) **Courts:** Defense counsels can take mobile computers in court. When the opposing counsel references a case which they are not familiar, they can use the computer to get direct, real-time access to on-line legal database services, where they can gather information on the case and related precedents. Therefore mobile computers allow immediate access to a wealth of information, making people better informed and prepared.

(III) **Companies:** Managers can use mobile computers to conduct critical presentations to major customers. They can access the latest market share information at any time and in anywhere. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can leverage competitive advantages.

(IV) **Emergency Services:** Ability to receive information on the move is vital where the emergency services are involved. Information regarding the address, type and other details of an incident can be dispatched quickly, via a Cellular Digital Packet Data (CDPD) system using mobile computers, to one or several appropriate mobile

units which are in the vicinity of the incident. Here the reliability and security implemented in the CDPD system would be of great advantage.

(V) **Credit Card Verification:** At Point of Sale (POS) terminals in shops and spinnakers, when customers use credit cards for transactions, the intercommunication required between the bank central computer and the POS terminal, in order to effect verification of the card usage that can take place quickly and securely over cellular channels using a mobile computer unit. This can speed up the transaction process and relieve congestion at the POS terminals.

(VI) **Stock Information Collation/Control:** In environments where access to stock is very limited i.e. factory warehouses. The use of small portable electronic databases accessed via a mobile computer would be ideal. Data collated could be directly written to a central database, via a Cellular Digital Packet Data (CDPD) network, which holds all stock information hence the need for transfer of data to the central computer at a later date is not necessary. This ensures that from the time that a stock count is completed, there is no inconsistency between the data input on the portable computers and the central database.

(VII) **Electronic Mail/Paging:** Usage of a mobile unit to send and read emails is a very useful asset for any business individual, as it allows him/her to keep in touch with any colleague as well as any urgent developments that may affect their work. Access to the Internet, using mobile computing technology, allows the individual to have vast arrays of knowledge at his/her fingertips. Paging is also evident here, giving even more intercommunication capability between individuals, using a single mobile computer device.

Mobile applications progressively affect the dispersion of information as well as business activities. They happen to have gained wide acceptance as a result of the increase in terms of

the want in supporting the mobile workforce and the quick expansion in the devices and wireless technologies for communication. Countless mobile applications deliver personal services such as sending and viewing email, browsing the world wide web (WWW), viewing traffic and weather reports, watching movies and chatting with others (El-Alfy, 2005).

Mobile Computing devices have been widely deployed in so many organizations to speed up their organizational activities, and hence to reduce the cost that they might likely incurred when using paper work.

Mobile computing has also been deployed in health care which began with reference tools that allowed clinicians easy access to guidelines, medical literature, and drug information databases, as well as transaction-based systems, which automate specific clinical and business tasks (Turisco, & Case, 2001). In addition there are other developments where mobile computing is use as an extension of a hospital information system (HIS) or practice management system, where mobile devices is used to provide both HIS access and specific functionality.

According to Turisco and Case (2001) given the immature market and continually advancing technology components, today's effective applications are those focused on tasks that require data access at the point of care but do not require sophisticated infrastructures to transfer data between the device and the organization's computer system. Taking health care for instance according to Turisco and Case (2001) they include prescription writing, charge capture and coding, clinical documentation, clinical decision support, medication administration, inpatient care solutions, and outpatient care solutions.

Mobile facilities and services seem to be an evident choice for tourism and travelling as the travelers are on the move, which is the first standard for mobile services to be relevant. However, centered on a study conducted by Carlsson, Carlsson, and Walden (2005) further elaborated that few users have conveyed their wish to use their mobile devices whenever possible. The travel and tourism industry have been undergoing many dramatic changes during the last decade, due to the possibilities offered by technology of the internet.

A Research study was conducted by Carlsson, Carlsson, and Walden (2005) which investigated mobile services for the hospitality industry. He founded that the services from mobile devices is the obvious choice for travel and tourism as they are one of the largest and most rapidly expanding industry in the world and one of the significant users of ICT. It seems to be an obvious choice as all travelers are on the move. The study is done by contrasting the problems with travelers' attitude and expectation in order to improve productivity of some key routines in the hospitality industry.

### 2.2.1 Benefits of Mobile Computing

Currently the major advantage of mobile computing over traditional systems is the mobility, where by it affords to access data and functions anywhere (Turisco, & Case, 2001).

Some of the benefits of Mobile Computing include:

(I) **Improved Decision Making:** Mobile computing enables you conduct business at the point of activity. The ability to collect, access, and evaluate critical business information quickly and facilitating decision making that can have an after reaching effect on your organizations ability to compete successfully.

(II) **Improved Customer Relation:** The success of a business can often be measured by its ability to satisfy customers. Mobile computers gives your field workers the ability to answer customers questions, check order status and provide other services anytime their customers are in need of them irrespective of where they may be.

(III) **Increased Productivity and Reduced Costs:** Mobile computing can lead to increased individual productivity, increased sales per sales person, more service calls per repair person, less time spent by professionals on administrative work, and much more, all of which ultimately translates into higher sales at lower cost. More so, on the spot invoice production in vehicles servicing can lead to shorter payment cycles and better cash flow. The table below can be used to deduce the potential benefits of using mobile computing devices in Health Care:

**Table 2.2: Potential Benefits from Health Care Mobile Computing Applications (Turisco, & Case, 2001).**

| Mobile Computing Application | Positive Financial Impact | Improved Documentation and Coding | Decreased Wait Times for Patients | Decreased Wait Time for MDs | Improved Workflow | Decreased Number of Manual Tasks/Phone | Improved MD Satisfaction | Decreased Variation/ Improved Care Quality |
|---|---|---|---|---|---|---|---|---|
| Alert Messaging / Communication | | | X | X | | X | X | |
| Charge Capture and Coding | X | X | | | X | X | | |
| Clinical Documentation | | X | | | X | X | | |
| Decision Support | X | | | | | | X | X |
| Lab Order Entry and Results Reporting | | | X | X | | X | X | |
| Medication Administration | | X | | | X | X | | X |
| Prescription Writer | X | | X | X | X | X | X | |

## 2.3 Wireless Application Protocol (WAP)

The collection of wireless application protocol and specification standard that allows mobiles

devices to communicate with the web server using the WAP browser as well as displaying the contents back on the mobile devices screen is what is known as Wireless Application Protocol (WAP), essentially, it is the protocol that allow mobile devices to access the internet (WapForum, 2002a).

Mobile computing requires the need to understand the concept of wireless networking which invariably has experienced remarkable growth during the last few years and has every indication of reaching even higher levels of subscription (Sollenberger, Seshadri, & Cox, 1999)

Kalkbrenner and Nebojsa (2001) elaborated that there are still many weaknesses in the current version of Wireless Application Protocol (WAP) that require in-depth investigation, in as much as there is a need to investigate every new technology arriving in the market to discover its benefit for use on daily basis. Presently, mobile devices have been extremely popular worldwide. Consequently, most users of mobile computing devices stand the chances to use them as regard doing their transactions anywhere at any point in time. Mobile devices market shares have grown up dramatically, for instance mobile phones where mobile commerce (m-commerce) attracts various relative companies such as mobile handset manufacturers to create technologies to make additional values for their mobile range (Amor, 2002).

According to the International Engineering Consortium (IEC) Wireless Application Protocol (WAP) is an application environment and set of communication protocols for wireless devices designed to enable manufacturer, vendor and technology independent access to the Internet (International Engineering Consortium, 2007).

Agreed with all the pleasures of mobile computing and the everyday friendship and

association with the Internet, it is not astonishing that there is some amount of misunderstandings about what wireless is and does.

According to Nylander (2004) he explained that in the early days of wireless web, several companies produced their own proprietary application protocol, this made the wireless web development to be followed by one company communication protocol standard which can only be viewed by mobile phone that use that standard, and as such, it lacks standardization which invariably hinder the growth of wireless web, more so, users were confused and developers were screaming for standardization.

Standardization is one of the most important aspects of wireless communications. WAP is intended primarily for Internet enabled digital phones, pagers and other handheld devices. It is designed to standardize development across different wireless technologies worldwide. In 1997, the Wireless Application Protocol (WAP) was developed by Nokia, Ericsson, Motorola and others to foster the emergence of the wireless Internet. It is designed to standardize development across different wireless technologies worldwide (Computing, 2000). Moreover, in June 2002, 350 member companies –involved WAP forum companies- joined together and formed the Open Mobile Alliance (OMA). They represent the world's leading mobile operators, device and network suppliers, information technology companies, application developers and content providers (Open Mobile Alliance (OMA), 2004).

According to analysts at Lehman Brothers Inc (Kustin, 2002), the number of wireless Internet access devices being utilized worldwide is expected to double annually from approximately 50 million units in the year 2000 to approximately 600 million units in the year 2004. Based on this data, recognizing the upcoming need to have pricing information and purchasing opportunities available for users of handled Internet access devices is essential for companies looking to become the most preferred suppliers of consumer goods on the Web. Moreover,

IEC (International Engineering Consortium, 2007) believes that the future for WAP will be bright; based on 75 percent of the world company's stand behind the mobile telephone market and the huge development potential of WAP.

### 2.3.1 WAP Architecture

Wireless Access Protocol entails a client and server methodology that compounds wireless network and internet technology. Consequently, the impetus for developing WAP was to spread Internet technologies to wireless networks, carriers and devices (Wapforum, 2002b).

WAP 1.0 was the first specification of WAP released in 1998 by WAP Forum. Trailed by WAP 2.0 which is a next-generation set of specifications that employed and supported improvements in the competences of the up-to-date wireless devices and Internet content technologies, in addition, WAP 2.0 delivers managed backwards compatibility to existing WAP content, applications and services that fulfill the previous WAP versions.

It was aimed to work on any mobile network standard such as Bluetooth, Infrared (IR), Wireless LAN (IEEE 802.11 protocol), or cellular networks such as General Packet Radio Service (GPRS), Global System for Mobile Communications (GSM) (Antovski, 2003; Cervera, 2002; & Kalliola, 2005).

There are layering concept in WAP such as that of the internet, which is known as the WAP protocol stack as depicted in figure 2.3.0 where each layers of the architecture is reachable by the layers above, as well as by other services and applications.

As depicted in figure 2.9 the WAP layer stack and internet OSI (International Standard Organization) layer stack. WAP stack consist of Wireless Application Environment (WAE),

Wireless Session Protocol (WSP), Wireless Transaction Protocol (WTP), Wireless Transport Layer Security (WTLS) and Wireless Datagram Protocol (WDP).

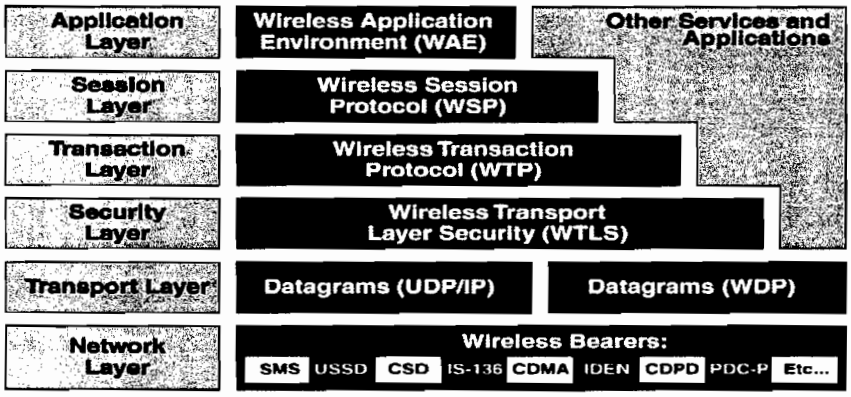



**Figure 2.9: WAP Protocol Stack (Wapforum, 2002a)**

### (I) Wireless Application Environment(WAE)

The WAE layer is where the protocol for the user interface resides, it also interact with Wireless Markup Language (WML), and WML is equivalent to the HTTP in the internet, WML Script and Wireless Telephony Application (WTA) to display content on the screen.

### (II) Wireless Session Protocol (WSP)

The WSP consist of two protocols that have to do with:

i. Work with WTP to make connection oriented session,

ii. Allow server to make connectionless oriented session (PUSH technology).

### (III) Wireless Transaction Protocol (WTP)

WTP layer is responsible to manage a transaction, it is also employed in the User Datagram Protocol (UDP) on the internet OSI (International Standard Organization) model, and it deals with three classes of transaction service which has to do with: unreliable one way request, reliable one way request and reliable two way request respond.

(IV) **Wireless Transport Layer Security (WTLS)**

Wireless Transport Layer Security deals with security data integrity and authentication protocol.

(V) **Wireless Datagram Protocol (WDP)**

WDP is a data transport protocol that manages the transmission; it also allows WAP protocol to adapt to any data communication protocol from network standard, and as such allowing WAP to communicate with any network standards.

## 2.4 Challenges of Mobile Computing

While the future of mobile computing in the context of next generation of future networks looks promising, there are many challenges still to overcome to make it a reality (Agrawal, & Famolari, 1999).

Mobile computing devices for instance notebooks, PDAs, smartphones and USB storage drives have become ubiquitous, and for a growing number of workers, their jobs would be quite challenging and difficult without the mobility provided by these devices. However, poorly managed mobile devices seriously increase the potential for security failures and breach of information.

Mobile devices should be protected against attacks on the network. Mobile devices such as notebooks running off-the-shelf of operating systems for instance are vulnerable to the same attacks as any other computer system, is as much as they need to function in external networks, such as, airport kiosks or coffee shops, and for that mobile devices have extra

stringent security needs. They can't rely on the organization's firewall for full protection. And the organization needs a means of managing security configuration, patch deployment and antivirus updates on their devices in the field. And for this the risk to users of wireless technology has increased exponentially as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. Currently, there are a great number of security risks associated with wireless technology. Some issues are obvious and some are not. At a corporate level, it is the responsibility of the IT department to keep up to date with the types of threats and appropriate counter measures to deploy.

According to Zhiming and Jingmei (2009) Security threats are growing in the wireless arena. Crackers have learned that there is much vulnerability in the current wireless protocols, encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has become much easier and more accessible with easy-to-use Windows-based and Linux-based tools being made available on the web at no charge. IT personnel should be somewhat familiar with what these tools can do and how to counter act the cracking that stems from them. Wireless threats come in all shapes and sizes, from someone attaching to your WAP (Wireless access point) without authorization, to grabbing packets out of the air and decoding them via a packet snuffer. Many wireless users have no idea what kind of danger they face merely by attaching a WAP to their wired network.

### 2.4.1 Security Threats and Attacks on Wireless Networks

Zhiming and Jingmei (2009) explained that Security threat refers to the dangers of the confidentiality, integrity, availability, or the legitimate use by a person to an event or a resource. Security threats can be divided into deliberate and accidental types.

Wireless Local Area Networks (WLAN) are increasing in popularity. They are being installed by businesses of all types, educational institutions, governments, and the military. WLANs provide users a significant mobility advantage as users can access their information in many locations, some of which are more conducive to collaboration. The freedom and mobility that WLANs promise, however, also present some serious security challenges. In the military domain, the department of defense transition from industrial-age to network-centric warfare brings with it technical challenges that are highly dependent and revolve around the successful implementation of a robust and secure wireless network of systems (Welch & Lathrop, 2003).

The airborne nature of WLAN transmission opens your network to intruders and attacks that can come from any direction. WLAN traffic travels over radio waves that the walls of a building cannot completely constrain complete information assurance risk assess men requires a focus on the threats against the three key components of assuring information. That is, the information system should protect against confidentiality, integrity, and availability (CIA) attacks (Welch & Lathrop, 2003).

Wireless threats come in all shapes and sizes, from someone attaching to your WAP (Wireless access point) without authorization, to grabbing packets out of the air and decoding them via a

packet snuffer. Many wireless users have no idea what kinds of danger they face merely by attaching a WAP to their wired network. This section discusses the most common threats faced by adding a wireless component to your network and they include:

#### 2.4.1.1 Traffic Analysis

According to Welch and Lathrop (2003) Traffic analysis is a simple technique whereby the attacker determines the load on the communication medium by the number and size of packets being transmitted, the source and destination of the packets and the type of packets. The assumption is that the payload of the packets is encrypted and the attacker cannot decrypt the payload. This leaves only the header and any trailer information visible to the attacker. The attacker only needs a wireless card operating in promiscuous (i.e. listening) mode and software to count the number and size of the packets being transmitted. A simple yagi or helical directional antenna provides an increased range at which the attacker may analyze traffic. Traffic analysis allows the attacker to obtain three forms of information and they include:

(I) Identifying that there is an activity on the network. Similar to standard radio communications, a significant increase in the amount of network activity serves as an indicator for the occurrence of a large event.

(II) The identification of information about the physical location of the wireless access points (APs) in the surrounding can also be acquired from traffic analysis. Except that the Access point is turned off, access points broadcast their Service Set Identifiers (SSIDs) in order to identify themselves to wireless nodes desiring access to the network. SSID is a parameter that must be configured in the wireless card's driver

software for any wireless station desiring access to a wireless LAN. By broadcasting this information, access points allow anyone in their area to identify them with simple locator software. If a directional antenna is used along with a Global Positioning System (GPS), an attacker may know not only that there is an AP(s) in the area, but may also obtain the physical location of the access point or the center of the wireless network. From a military standpoint, this is the same technique used in triangulating radio communications or field artillery batteries for the purpose of counter fire.

(III) Identification of the type of protocols being used in the transmission through traffic analysis. This knowledge is obtained based on the size, type and the number of packets in transmission over a period of time. A simple example of this attack is the analysis of a Transmission Control Protocol (TCP) three-way handshake. TCP synchronizes the communication between two end nodes by transmitting a series of three packets. The sender transmits a synchronize (SYN) packet to let the receiver know it wants to communicate, to provide it with the sender's initial sequence number, and to pass other parameters used in the protocol. The receiver then replies with its initial sequence number an acknowledgement of the original sender's sequence number (SYNACK). Finally, the original sender transmits an acknowledgement of the receiver's initial sequence number (ACK) and then the transmission of application data between the two nodes may commence. Each packet used in the three way handshake is a fixed size in terms of the number of bytes transmitted.

#### 2.4.1.2 Passive Eavesdropping

In this attack according to Welch and Lathrop (2003) the attacker passively monitors the wireless session and the payload. If the payload is encrypted, this includes breaking the

encryption to read the plaintext. The only precondition is that the attacker has access to the transmission.

The attacker can gain two types of information from passive eavesdropping. The attacker can read the data transmitted in the session and can also gather information indirectly by examining the packets in the session, specifically their source, destination, size, number, and time of transmission. The impact of this type of attack is that not only is the privacy of the information compromised, but the information assembled is an important precondition for other, more damaging attacks. According to Welch and Lathrop (2003) figure 2.10 was used to explain passive eavesdropping.

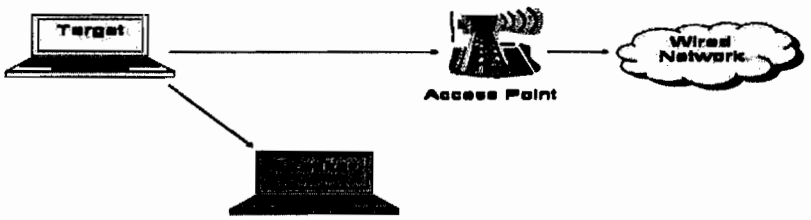



**Figure 2.10: Passive Eavesdropping (Welch & Lathrop, 2003)**

### 2.4.1.3 Active Eavesdropping

The active eavesdropping technique according to Welch and Lathrop (2003) involves the attacker injecting data into the communication to help decipher the payload. The attacker monitors the wireless session as described in passive eavesdropping. Unlike passive eavesdropping, however, during active eavesdropping, the attacker not only listens to the wireless connection, but also actively injects messages into the communication medium in order to assist her in determining the contents of messages. The preconditions for this attack

are that the attacker has access to the transmission and has access to either part of plaintext such as a destination IP address or the contents of the entire payload.

These attacks can take two forms: the attacker can modify a packet or can inject complete packets into the data stream. Since WEP uses a cyclic redundancy check (CRC) to verify the integrity of the data in the packet, an attacker can modify messages (even in encrypted form) so that changing data in the packet (i.e. the destination IP address or destination TCP port) cannot be detected. The attacker's only requirement is to determine the bit difference between the data they want to inject and the original data.

An example of active eavesdropping with partially known plaintext is IP Spoofing. The attacker changes the destination IP address of the packet to the IP address of a host she controls. The access point does the decryption prior to forwarding the altered packet on to the attacker's host.

#### 2.4.1.4 Unauthorized Access

Unauthorized Access is different from any of the previous attacks that we have discussed in that; it is not directed at any individual user or set of users on the WLAN. It is directed against the network as a whole. Once an attacker has access to the network, she can then launch additional attacks or just enjoy free network use. Although free network use may not be a significant threat to many networks, access is a key step in Address Resolution Protocol (ARP) based man-in-the-middle attacks (Welch, & Lathrop, 2003). Figure 2.11 was used to explain an unauthorized access threat.


**Figure 2.11: Unauthorized Access (Welch & Lathrop, 2003).**

As a result of the physical properties of Wireless LANs, intruders or attackers will always have access to the wireless component of the network as shown in figure 2.11. Considering some wireless security architectures, this will also grant the attacker access to the wired component of the network. In other architectures, the attacker must use some technique like MAC addresses spoofing to gain access to the wired component of the network.

### 2.4.1.5 Man-In-The-Middle Attack

If the packets being transmitted are encrypted only at the network layer (layer 3), then the attacker can obtain the header information from the data link layer (layer 2) and layer 3. A VPN or IPsec security solution entails such a countermeasure. Although these solutions protect the users from a direct confidentiality attack against the application data, it does not deny indirect confidentiality attacks such as man-in-the-middle attack as shown in figure 2.12 session hijacking, or replay attacks (Welch, & Lathrop, 2003).

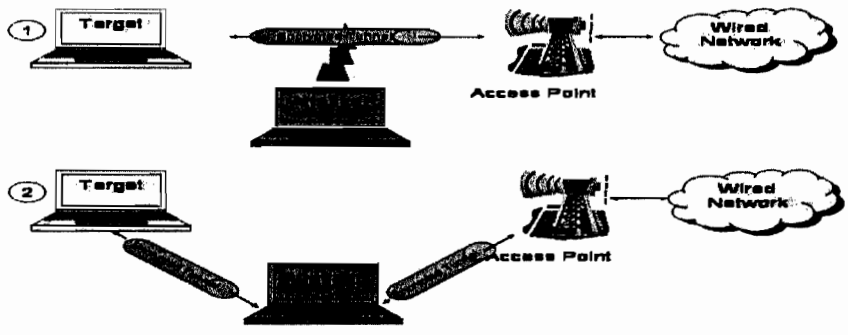



Figure 2.12: Man-in-the-Middle Attack (Welch & Lathrop, 2003).

A man-in-the-middle attack as shown in figure 2.12 can be used to read private data from a session or to modify the packets thus violating the integrity of a session. This is a real-time attack, meaning that the attack occurs during a target machine's session. The data may be read or the session modified as it occurs. The attacker will know the contents of the message prior to the intended recipient receiving it, or change the message end route.

Differences on this attack method are based on the security instrument and mechanisms employed. The more security mechanisms in use the more security mechanisms that the attacker will have to sabotage when reestablishing the connection with both the target and the access point. In the absence of encryption or authentication in use the attacker establishes a rogue access point. The target unsuspectingly associates to the rogue which acts as a proxy to the actual wireless network. In order words, if authentication is put in place the attacker must overcome the authentication mechanism to establish new connections between herself and the target and herself and the access point. If encryption is been put in place in, the attacker must also overcome the encryption to either read or modify the message contents. Since 802.11 authentications are not mutual between the access point and the client, and the default encryption (WEP) is easy to crack, man-in-the-middle attacks are somewhat trivial on 802.11 networks.

#### 2.4.1.6 Address Resolution Protocol (ARP)

ARP attacks are a particularly dangerous subset of man-in-the-middle attacks because these attacks can be directed against targets on the wired component of the network, not just wireless clients. The attack can involve either bypassing the authorization mechanism, if it

exists, or providing false credentials. The ARP attack differs from the other attack techniques in that the credentials may in fact belong to a valid user. The attacker is only gaining access to the network and is not masquerading as the target. This may be an ambiguous distinction but we find it useful when analyzing authorization technologies (Lynn, Mike, & Baird, 2002; Schwartz, & Ephraim, 2002; Colubris, 2002; Borisov, Nikita, Goldberg, &Wagner, 2001; Mishra, Arunesh, &Arbaugh, 2002 ).

The Address Resolution Protocol (ARP) maps the Media Address Controller (MAC) address (Layer 2) of a network node to the Internet Protocol address (Layer 3). Altering the mapping of the MAC address to IP address allows an attacker to reroute network traffic through her machine. With the session passing through the attacker's computer the attacker can read plaintext, collect encrypted packets for later decryption, or modify the packets in the session. ARP cache poison attacks are contained by routers but a great deal of damage can be done with a successful ARP Cache Poisoning attack (Whalen, Sean, Fleck, Bob, & Dimov, 2002; Carey, & Allan, 2001).

To carry out a successful attack the attacker must have access to the network but nothing else. The attacker sends a forged ARP reply message that changes the mapping of the IP address to the given MAC address. The MAC address is not changed just the mapping. Once the cache has been modified the attacker can act as a Man-In-The-Middle between any two hosts in the broadcast domain. This is illustrated in Figure 2.13 where an attacker on a wireless client has access to sessions between two wired hosts (Welch, & Lathrop, 2003).

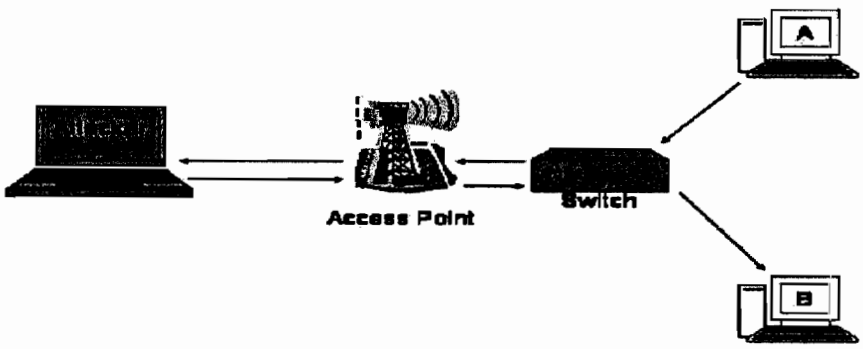



**Figure 2.13: ARP Attack (Welch & Lathrop, 2003).**

According to Welch and Lathrop (2003) they mentioned that denying this attack, technique is an absolutely vital step in designing the security architecture. Denying access to the WLAN limits the attacker's possibilities for further attack. Defending against unauthorized access will make successful attack on the integrity of the WLAN much more difficult. We have separated ARP redirection attacks from Man-In-The-Middle attacks because ARP redirection does not require that the attacker establish sessions with the target and the network. ARP attacks can be a way of performing traffic analysis or passive eavesdropping.

### 2.4.1.7 Session High-Jacking

An attack against the integrity of a session is what is known as Session High Jacking. An authorized and authenticated session will be taken away from the proper owner by an attacker, and as such, the target knew quite alright that it no longer has access to the session but may not be aware that the session has been taken over by an attacker. The target may attribute the session loss to a normal malfunction of the WLAN. Once the attacker owns a valid session she may use the session for whatever purposes she wants and maintain the session for an

extended time. This attack occurs in real-time but can continue long after the victim thinks the session is over.

According to Mishra, Arunesh, and Arbaugh (2002); Schwartz, and Ephraim (2002); Skoudis and Ed (2002) to successfully execute Session High Jacking the attacker must accomplish two tasks. First she must masquerade as the target to the wireless network. This includes crafting the higher-level packets to maintain the session, using any persistent authentication tokens and employing any protective encryption. This requires successful eavesdropping on the target's communication to gather the necessary information as shown in step one of Figure 2.14. The second task or step the attacker must perform is to stop the target from continuing the session. The attacker normally will use a sequence of spoofed disassociate packets to keep the target out of the session as shown in Figure 2.15.

**Step 1**

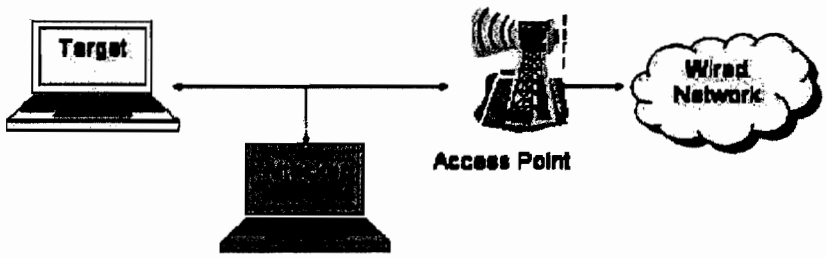



**Figure 2.14: Session High-Jacking (Welch & Lathrop, 2003).**

Step 2

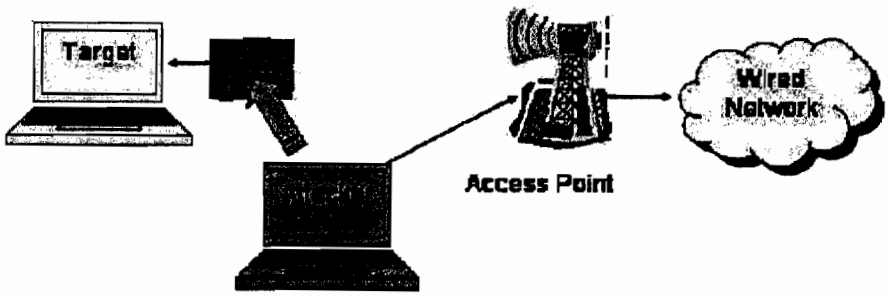



**Figure 2.15: Session High-Jacking (Welch & Lathrop, 2003).**

### 2.4.1.8 Replay Attack

According to Krishnamurthy, Prashnt, Kabara, Tanapat (2002); Moioli, Fabio (2000); Borisov, Nikita, Goldberg and Wagner (2001) replay attacks are also aimed at the integrity of the information on the network if not necessarily the integrity of a specific session. Replay attacks are used to gain access to the network with the authorizations of the target, but the actual session or sessions that are attacked are not altered or interfered with in anyway. This attack is not a real-time attack; the successful attacker will have access to the network sometime after the original session(s).

In a replay attack as depicted in figure 2.16 the attacker captures the authentication of a session or sessions. The attacker then either replays the authenticated session at a later time or uses multiple sessions to synthesize the authentication part of a session. Since the session was valid, the attacker establishes an authenticated session without being privy to any shared secrets used in authentication. Without further security mechanisms the attacker may interact with the network using the target's authorizations and credentials. If the WLAN employs encryption that the attacker cannot defeat the attacker may still be able to manipulate the

WLAN by selectively modifying parts of the packet to achieve a desired outcome (Krishnamurthy, Prashnt, Kabara, Tanapat 2002; Moioli, Fabio 2000; Borisov, Nikita, Goldberg and Wagner 2001).

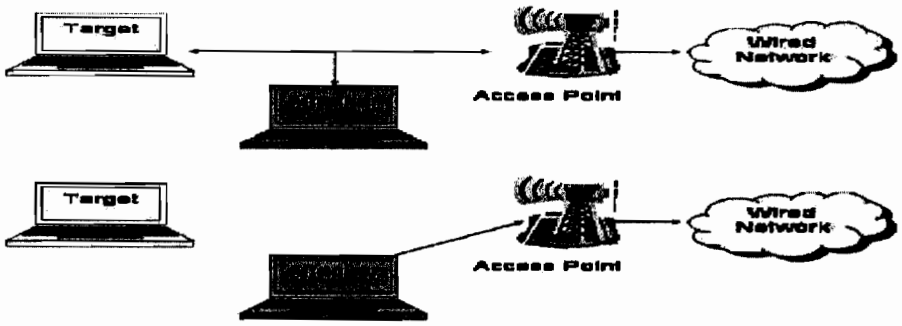



**Figure 2.16: Replay attack (Welch & Lathrop, 2003)**

### 2.4.1.9 Denial of Service

According to Blackert, Gregg, Castner, Kyle, Hom and Jokerst (2003); Wang and Schulzrinne (2004) Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus preventing legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be

performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic (Pathan, Lee & Hong, 2006).

#### 2.4.1.10 Sybil Attack

In most instance, the sensors in a wireless sensor network might need to work together to accomplish a task, hence, they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes as depicted in figure 2.17. This type of attack where a node forges the identities of more than one node is the Sybil attack (Douceur, 2002; Newsome, Shi, Song, & Perrig, 2004).

Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection (Newsome, Shi, Song, & Perrig, 2004), as cited in (Pathan, Lee, & Hong, 2006). Mostly, any peer-to-peer network, take for instance ad hoc and wireless networks is vulnerable to Sybil Attack. Nevertheless, as Wireless Networks can encompass some categories of gateways or base stations, such attacks could be stopped by employing well-organized protocols. Douceur (2002) presented that, without a reasonably centralized authority, Sybil attacks are continuously possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of Sybil nodes in a network is not so easy.

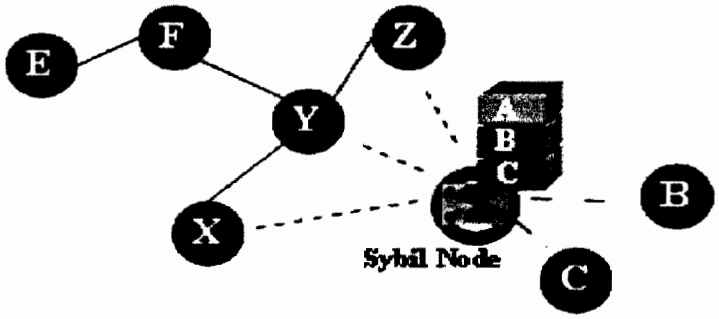



**Figure 2.17: Sybil Attack (Pathan, Lee, & Hong, 2006)**

At this juncture, it should be noted that Wireless LAN such as Mobile Computing devices are prone and vulnerable to risk, threats and attacks when deployed or used, and for these reasons they require strong security mechanisms for their protection due to their open medium, and as such, if strong security mechanisms are not put in place it might affect the system performance, as well as resulting into a negative impact in the Quality of Service (QoS) of communication (Agarwal, Wang, & McNair, 2005).

## 2.5 Network Security

Network security is a critical concern for enterprises, government agencies, and organizations of all kind. Today's advanced threats demand a systematic approach to network security. In many businesses enhanced security is not an option but its mandatory where organizations such as financial institutions, health care providers, and federal agencies are strictly advised to implement stringent security programs to protect digital assets (Ashley, 2006).

In general, Security according to Kurose and Ross (2008) refers to methods of guaranteeing that information and data stored in the system cannot be conceded by any individuals without authorization except with the use of password and username for authentication.

Data encryption is the translation of data into a form that is meaningless without any interpreting device.

A password is a secret word or phrase usually made use of by users to gain access to a system by authenticating themselves to that particular program or system.

Network Security is a continuing process of defining security policies, implementing proactive security measures and enforcing them, as well as monitoring the network to obtain visibility, identifying and correlating irregularities, mitigating threats and reviewing what occurred in order to modify and improve the security posture, as illustrated below in figure 2.18.

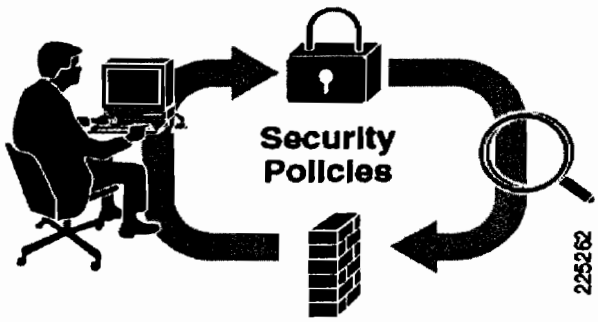



**Figure 2.18: The Security Process (Cisco Validated Design, 2008)**

### 2.5.1 Security Challenges in Wireless Networks

The rapid increase and growth of networking, such as wireless technologies, has led to increase in security risks (Corral, Cadenas, Zaballos, & Cadenas, 2005). Many of these

risks are due to hacking, as well as inappropriate uses of network resources. WLANs allows for unique security challenges because they are vulnerable to dedicated and particular attacks (Corral, Cadenas, Zaballos, & Cadenas, 2005). Many of these attacks exploit technology weaknesses since 802.11 WLAN security is relatively new. There are also many configuration weaknesses since some companies are not using the whole security features of WLANs on all their equipment. Finally, there are policy weaknesses. When a company does not have a clear policy on wireless usage, employees may set up their own Access Points (AP), which is rarely secure (Corral, Cadenas, Zaballos, & Cadenas, 2005).

Access to wireless network can be an unlimited threat to network security. Most WLANs have little or no limitations, once connected to an AP, an attacker can easily travel an unsecured internal network and even compromise wired network security. Compromising only one node or presenting a nasty node may upset the viability of the entire network (Yang, Xie, & Sun, 2004). A policy as regard security must recognize the security objectives of wireless network in an organization, document resources to be protected and recognize network infrastructure. An active policy as regard wireless security works to guarantee that network assets of the organization are protected from unauthorized access. Similarly, network security analysis must organize different springs of information to support effective security models (Dawkins, & Dale, 2004). Shuyao, Youkun, Chuck and Kai (2004) reported that there is a great security challenge on the nature of the wireless networks, which poses as a clog for the system security designers which could be traced to the following possible reasons:

(I) The wireless network is more prone to attacks ranging from passive eavesdropping to active interfering.

(II) The lack of an online Confidentiality and Authentication or Trusted Third Party adds the difficulty to deploy security mechanisms.

(III) Mobile devices tend to have limited power consumption and computation capabilities which make it more vulnerable to Denial of Service attacks and incapable to execute computation.

(IV) In wireless networks there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, however there should be a consideration for both the internal and external attacks in wireless networks, in as much as the internal attacks are more difficult to deal with.

**(V)** Node mobility enforces frequent networking reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between stale routing information and faked routing information. There are five main security services for wireless mobile computing devices and they are authentication, confidentiality, integrity, non-repudiation, and availability.

### 2.5.2 Wireless Network Security

There have been so many focus in recent times concerning security aspects of existing WI-FI

(IEEE 802.11) wireless LAN systems. The exponential growth and increase as regard the deployment of these systems into a huge range of networks and for a wide variety of applications brings about the necessity to support security solutions that meet the requirements of wide variety of users.

The main aspect that makes wireless security different than security of wired networks is the uncontrollability of physical access due to transmission of data with radio waves. This fact makes 802.11 networks vulnerable to eavesdropping.

According to Tillwick and Olivier (2004); Borisov, Goldberg and Wagner (2001) securities in wireless networks as the name implies must ensure that the respectives goals of securing a wireless networks such as mobile computing is fully achieved, which has to do with the following:

(I) **Confidentiality**: This has to do with ensuring that only the sender and the intended receiver is able to understand the content of the transmitted message, basically to avoid eavesdropping or interception of transmitted messages (Kurose, & Ross, 2008).

(II) **Authentication**: This is normally used by both the sender and receiver to endorse the identity of the other party involved in the communication, that is, to endorse that the other party is indeed who he or she claims to be (Kurose, & Ross, 2008).

(III) **Data Integrity**: The content of the message sent and received must be protected, in such a way that the messages are not damaged, deliberately changed or altered, or tampered with during transmission (Borisov, Goldberg, & Wagner, 2001).

(IV) **Access Control:** The security deployed must ensure that all unauthorized traffic or contents should not have access to the wireless network infrastructures (Borisov, Goldberg, & Wagner, 2001). In other words, network **access control clarifications protect the network by certifying that endpoints meet defined security standards before they are permitted to access the network** (Ashley, 2006).

Nevertheless, all the above security goals are very important in order to achieve adequate security implementation in mobile computing devices which cannot be fully achieved using un-layered security approaches as a result of their weaknesses when used in protecting wireless devices, some of which are explained below.

## 2.6 Weaknesses in UnLayered Security Architectures

According to Orinoko (2003) deploying Traditional Security approaches to secure wireless devices such as mobile computing can be broken into two parts, which has to do with Authentication that can be achieved using Medium Access Control (MAC) mechanism, and encryption which can be achieved using 802.11 Wired Equivalent Privacy (WEP), where Authentication can be used to identify a wireless client to an access point, and an access point to a wireless client, while Encryption algorithms ensure that it is not possible for an intruder to intercept and decode data.

### 2.6.1 Authentication

Prior to transmitting data a client must authenticate and establish an association with an Access Point (AP). An association is merely a connection between the client and an AP (Craiger, 2002). The 802.11 standard offers two types of authentication Open systems authentication and the Shared-Key authentication, where the open systems authentication is the default for many Aps and a requirement of the standard, it permits any clients to associate with an AP in as much as the Service Set Identification (SSID) are equal (Craiger, 2002).

Access to the Wireless LAN is normally controlled by the Shared-key authentication with the use of a shared key, which is used to provide effective stringent access to the network resources (Craiger, 2002).

Media Access Control (MAC) authentication of wireless clients can be used to support access points, where only traffic from authorized MAC addresses will be permitted through the access point. The access point will decide if a specific MAC address is legal by examining it against either a Remote Authentication Dial-In User Service (RADIUS) server external to the access point or against a database within the nonvolatile storage of the access point. This is somewhat a weak authentication mechanism because it can be sidestepped, and because authentication is one-sided. It can be by-passed for two reasons. One, software exists to alter or change the MAC address of some 802.11 cards. Two, authentication is tied to the hardware that a person is using and not to the identity of the user. Thus, it could be imaginable and possible to steal a legitimate user's PC and gain illegal access to a network. Unilateral on one-sided authentication means that the user does not authenticate the access point, but the access point authenticates the user, that is, there is no two-way authentication, this unilateral authentication is a problem because an unsuspecting user could associate to a rogue access point and begin passing network usernames and passwords through the illegitimate access

point. This would allow hacker to capture the unsuspecting user's credentials to gain access to other network resources (Orinoko, 2003; Craiger, 2002). According to Craiger (2002) a shared key authentication diagram can be depicted in figure 2.19.

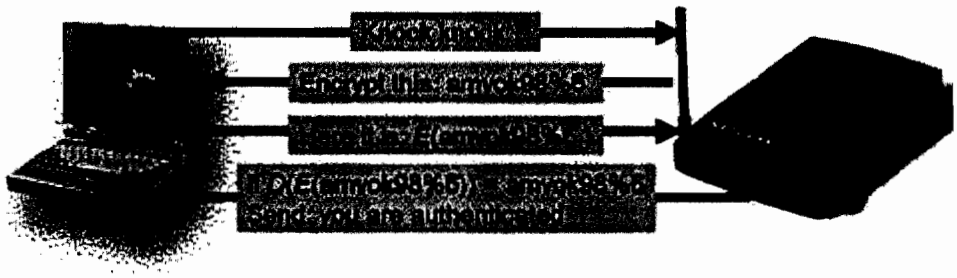


**Figure 2.19: Shared-Key Authentication Process (Craiger, 2002)**

Nevertheless, there are so many weaknesses concerning the use of open authentication. If there is anyone who is familiar with the SSID, that person can gain network access, to be candid, it is simple and very easy to discover an APs SSID in as much as each AP sends beacon frames which contain its SSID that can be readable by human (Arbaugh, Shankar, & Wan, 2001).

Except sharing network resources with everyone is your hubby, open authentication should not be used.

The Shared-key authentication is more secure compare to the Open authentication, but still problematic. It is not possible to authenticate and track an individual user since all clients use the same key. Likewise, the key used for WEP is the same used as the shared-key for authentication. Consequently, by stealing one key an enemy kills the well-known two-birds, and now has access to authentication, as well as encryption and decryption. Also note that an AP authenticates a user, but a user does not and cannot authenticate an AP.

### 2.6.2 Encryption

Presently, much attention has been paid recently to the fact that Wired Equivalent Privacy (WEP) encryption defined by 802.11 is not an industrial strength encryption protocol (Orinoko, 2003). A link-layer security protocol that is not required but specified, by the 802.11 standard is the WEP. WEP uses RC4 stream cipher, a symmetric cipher where an identical key is used for both encryption and decryption, where the most widely used stream cipher in software applications is RC4 (Fluher, Mantin & Shamir, 2001).

Consequently, The term 'wired equivalent' denotes that the security provided by WEP in a wireless LAN is intended to be roughly equivalent to what one would expect in a wired LAN (Erten, & Tomur, 2004).

Wired Equivalent Privacy (WEP) as depicted in figure 2.20 is designed mainly to mitigate these weaknesses in wireless LAN security by aiming to provide privacy of transmitted data using encryption and trying to prevent tampering of messages by means of integrity checking. RC4 algorithm is used for encryption with 64 or 128 bit long keys, 24 bits of which is a random number known as Initialization Vector (IV), and CRC-32 integrity checking algorithm is used for message integrity, the figure below graphically illustrate WEP.

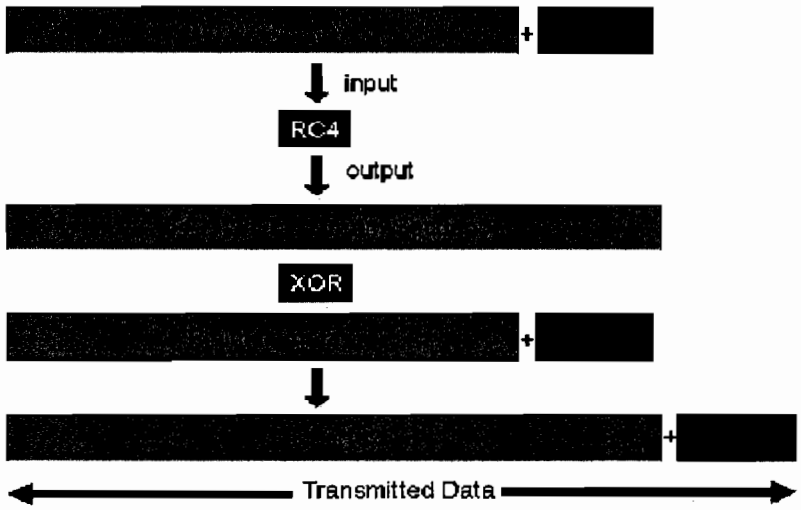



**Figure 2.20: Wired Equivalent Privacy (Loeb, 2001)**

The above Traditional 802.11 security stated earlier on are considered to be inadequate in protecting or securing wireless devices such as mobile computing for the fact that intruders can breach or compromise the above security architectures in no small measures as a result of their weaknesses. For instance, WEP has a lot of vulnerabilities in both its encryption and integrity checking procedures, as a result of insufficient IV space, an unauthorized person can read the transmitted data using decryption dictionaries (Walker, 2000), or the WEP key can be cracked by a person by making use of the weaknesses in generation of key streams (Fluhrer, Martin, & Shamir (2001). Likewise, weaknesses of CRC-32 algorithm against attacks can be exploited by malicious people to alter packets or even insert fresh messages into the network (Borisov, Goldberg, & Wagner, 2001).

According to Borisov, Goldberg, and Wagner (2001) WEP was intended to enforce three security goals which has to do with:

(I) Confidentiality, used in preventing eavesdropping using encryption algorithm,

(II) Access control to discard improperly encrypted packets using authentication mechanisms, and

(III) Data integrity for preventing transmissions which has been tampered with the use of data checksum.

WEP has several weaknesses that have been extensively known and distributed. These weaknesses allow passive or active attacks on wireless transmissions, by allowing attackers to decrypt information or alter information into the transmissions. Most of these attacks depend on the ability of the attacker to monitor the 2.6 GHz radio frequencies and interpret the 802.11 physical layers into human readable form (Erten, & Tomur, 2004).

This is honestly easy to achieve, using a laptop or handheld device for instance, Compaq, as well as a wireless NIC capable of running in immoral approach, and easily available sniffer software capable of interpreting the packets into human readable (Erten, & Tomur, 2004). Another WEP weakness has to do with the IV collision, where IV is reused at some point in a wireless transmission, more so, it is also prone to weaknesses as regard the its popular stream ciphers where two packets can be decrypted despite the fact that they were encrypted with the same IV (Borisov, Goldberg, & Wagner, 2001).

There are other weaknesses concerning WEP such as the RC4s weak key scheduling, that typically permits keys to be predicted centered on the first few packets that was transmitted (Fluher, Mantin, & Shamir, 2001). Nevertheless, integrity check value algorithm concerning linearity that creates the CRC data fingerprint permits an invader to flip the bits on encrypted data basically to ascertain how the CRC value changes, which may create or provide clues as to the original plaintext (Arbaugh, 2001)

Misplacing a key management mechanism, errors of shared key authentication, as well as difficulties of authenticating access points are the other weaknesses of deploying un- layered

securities for mobile computing devices of conventional 802.11security( Arbaugh, Shankar, & Wan, 2002).

Temporal Key Integrity Protocol (TKIP) was developed in lieu of the security blemishes in the area of data encription. TKIP uses the same encryption algorithm as WEP that is RC4. Nevertheless, to guarantee that encryption keys are not used again, Initialization Vector's length is increased to 48 bits, more so MAC address of the client is used in key stream generation.

### 2.6.3 Strong Authentication (802.1x)

As a result of the drastic growth in mobile computing usage, and the weakness of current security protocols, new and better security mechanisms are required to protect wireless transmissions. One of these is the relatively new IEEE 802.1x standard.

The Working Group of the IEEE 802.11 passed the 802.1x standard in 2001 to advance upon the security stated in the original 802.11 standard (IEEE, 2001).

802.1x was envisioned to offer strong authentication, access control, and key management (Mishra & Arbaugh, 2001), and permit mobile computing to rule by permitting integrated authentication of wireless users or stations (Geier, 2002; Roshan, 2001).

802.1x is centered on a surviving authentication protocol known as the Extensible Authentication Protocol (EAP), where is an extension of point-to-point protocol (PPP) itself. 802.1x is not knotted to any precise networking arrangement, in other words, it serves as the

heart for authenticating users to the physical network, regardless of the underlying network protocols. Nevertheless, 802.1x maps EAP to the physical medium, regardless of whether it is Token Ring, wireless LAN or Ethernet (Erten, & Tomur, 2004). Consequently, it also supports numerous authentication procedures, which has to do with one-time passwords, token cards, certificates, and public key authentication (Geier, 2002; Roshan, 2001).

802.1x is a port based authentication framework used with Extensible Authentication Protocol (EAP) in a wireless LAN, and also serves as mutual authentication between clients and access points via an authentication server (Erten, & Tomur, 2004).

IEEE 802.11x standard is another enhancement to provide improved security for wireless LANs such as mobile computing devices. 802.1x is normally used for dynamic distribution of encryption keys, which is not possible in traditional WEP (Erten, & Tomur, 2004).

It should be noted that the 802.1x standard provides for authentication only, and as such the standard does not state the exact type of authentication or any type of encryption. However, as of June 2002 some vendors offer proprietary versions of dynamic key management using 802.1x as a delivery mechanism. As depicted in figure 2.21 through dynamic key exchange the authentication server is capable of returning session keys to the AP together with the message accepted (Geier, 2002).

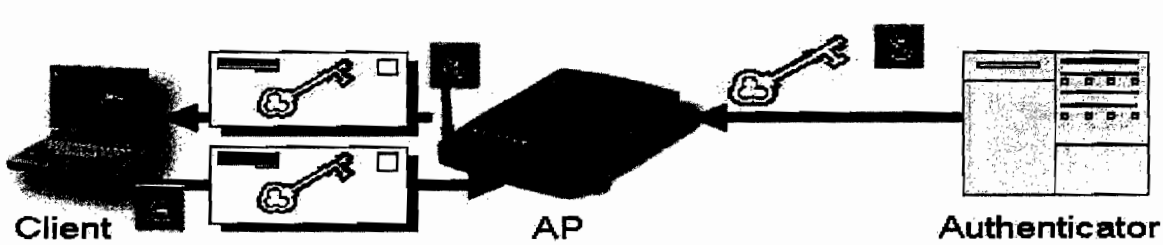



**Figure 2.21: 802.11x using Dynamic Key Session (Geier, 2002).**

It should be noted that 802.1 x authentications consist of three main mechanisms, that is, a client, an authenticator that has to do with the Access Point, and the authentication server.

The authentication server is usually a Remote Authentication Dial-In User Service (RADIUS) server, which is not specifically required by the standard (Geier, 2002).

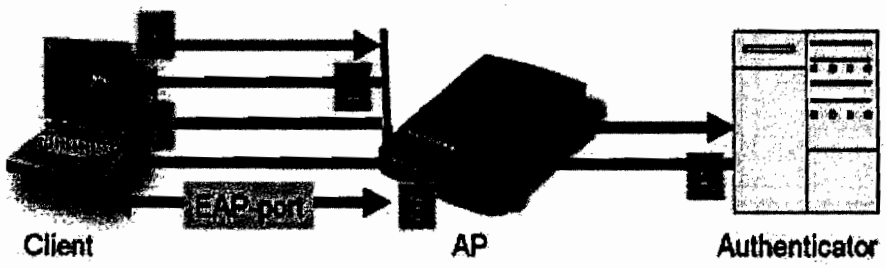



**Figure 2.22: 802.11x Authentication Process (Geier, 2002).**

However, the 802.1x protocol has its own weakness as well and as a result of this it tend not to be a guaranteed means for providing security for wireless LAN such as mobile computing based on Cisco published "Cisco Security Advisory: Catalyst 5000 Series 802.1x Vulnerability" in April, 2001 concerning a problem with its own 802.1x implementation (Cisco, 2001). According to some researchers at the University of Maryland, they found out that 802.1x is vulnerable to session hijacking as shown in figure 2.23 as well as man-in-the-middle attacks (Mishra & Arbaugh, 2001; Connolly, 2002; Schwartz, 2002).

According to Cole (2002) Session hijacking is when an attacker takes control of an existing or current session, which invariably means that the attacker is relying on an existing authenticated connection to obtain access to network resources.

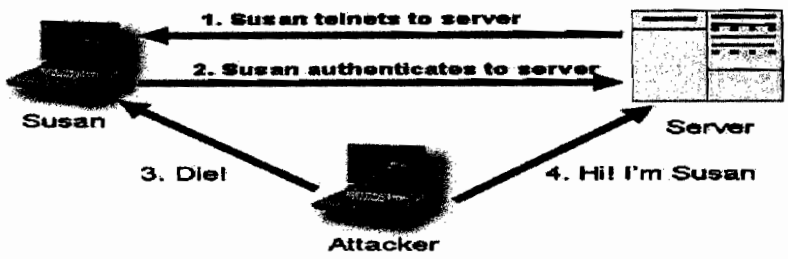



**Figure 2.23: 802.11x Session Hijacking (Cole, 2002).**

The figure above shows that the attacker delays until Susan (a valid user) authenticates, then murders or blocks Susan's connection which can be done through various forms of denial of service attacks (Cole, 2002), and successively pretends to be Susan. This necessitates the attacker spoofing the authenticated user's IP address in order to maintain the connection.

Likewise, Mishra & Arbaugh (2001) clarified session hijacking in the perspective of an authenticated 802.1x connection as follows:

(I) The hacker pauses for someone to authenticate successfully.

(II) The attacker sends a quit message, by spoofing it to make it looks as if it came from the AP.

(III) The client thinks they have been sent parking, whereas the AP thinks the client is still out there.

(IV) As long as transmissions are not encrypted the attacker can start using that connection claiming to be the valid user.

Consequence to the above, neither traditional 802.11 security nor their improvements is adequate for satisfying the necessities of a secure network such as privacy, integrity and authentication. However, some serious issues concerning network security of organization are left totally untouched, such as access control and authorization, that a required to control access to some critical part of the network resources and granting effective and proper level of

access rights, are strictly impossible to implement using security approaches made mentioned earlier on (Erten, & Tomur, 2004).

Nonetheless, wireless network security is an important phenomenon for businesses, government agencies, and organizations of all kinds to be taken into consideration (Ashley, 2006). Adequate security deployment is not voluntary but mandatory for organization such as financial institutions, providers of health care basically to protect their digital assets from intruders (Ashley, 2006).

According to Ashley (2006) deploying wireless network securities according to professionals should be done in terms of "work factors" which is an important concept when implementing wireless network security using layered security architecture. Nevertheless, work factor is the energy required by an intruder to compromise several security actions, which in turn permits the network to be successfully breached.

A network with a high work factor is problematic to break into, while a network with a low work factor can be compromised easily with fewer difficulties. If intruders got to discover that your network has a high work factor, which is an advantage of the layered architectural approach, the intruders might probably go for a low work factor wireless network that is less secure, such as un-layered security architectural (Ashley, 2006).

At this juncture, it should be noted that today's advanced threats require a methodical means to wireless network security which has to do with securing wireless network using layered security approach (Erten, & Tomur, 2004).

## 2.7 Layered Security Approach

Layered security also known as layered protection used by Information Technology security experts, information protection experts, and software security sellers is the process of leveraging several different point security solutions, filtering systems, and observing strategies to secure information technology resources and data (Farouzan, & Fegan, 2007).

A layered defense according to Nortel (2007) uses many approaches to security implementation at several areas within a network, where the approach eliminates single points of security failure in order to secure enterprise information assets.

### 2.7.1 Layered Security Approaches

According to Ashley (2006) layered security approach is a technical strategy deployed in promoting adequate processes at several levels within an organization's network infrastructure. However, the layered security approach according to Ashley (2006) centers on preserving appropriate security measures and procedures at five different levels within your wireless network environment, but for the scope of this project we will cover only the Network Layer as regard Access Control (Authorization) and Authentication levels as shown in figure 2.24.


**Figure 2.24: Proposed Layered Security Approach (Ashley, 2006)**

i. **Perimeter Security Level**: This level stands as the first defense from outside an un-trusted wireless network, that is the region where your wireless network ends and as such where the internet begins.

ii. **Network Security Level**: This level stands as the second defense for the organization's internal wireless LAN and Wide Area Network.

iii. **Host Security Level**: This level has to do with the individual devices, such as laptops, PDA's, servers, routers, etc., on the network that must be configured appropriately to avoid security holes.

iv. **Application Security Level**: This is the level where applications are properly monitored and protected in order to ensure that there is an effective provision of easy access to confidential data and records.

v. **Data Security Level**: This security level is normally used by organization to monitor or govern who has access to data, what users are authorized to do with the data, and who has the final obligation for its integrity and protection.

The above model usually called Still Secured Best Practices approach had been into deployment by organizations since 2006 and will serve as a basis for achieving our result as regard safeguarding mobile computing due to the fact that it was widely accepted and deployed now by much organization to safeguard, secure and protect their digital asset and to reduce their exposure to any unknown catastrophic network breach.

### 2.7.2 Layered Security Approach for Wireless Networks

Neither the traditional 802.11 security nor their improvements is prominent for achieving the requirements of a secure network such as data integrity, privacy and authentication, for the fact that the fundamental issues governing enterprises level network security had been left unfulfilled, in likes of access control and authorization that are needed to monitor access to some critical part of the network at large and can best be achieved using a layered security approach (Erten, & Tomur, 2004). According to Erten and Tomur (2004) figure 2.25 was made use of to explain security method using a layered approach.

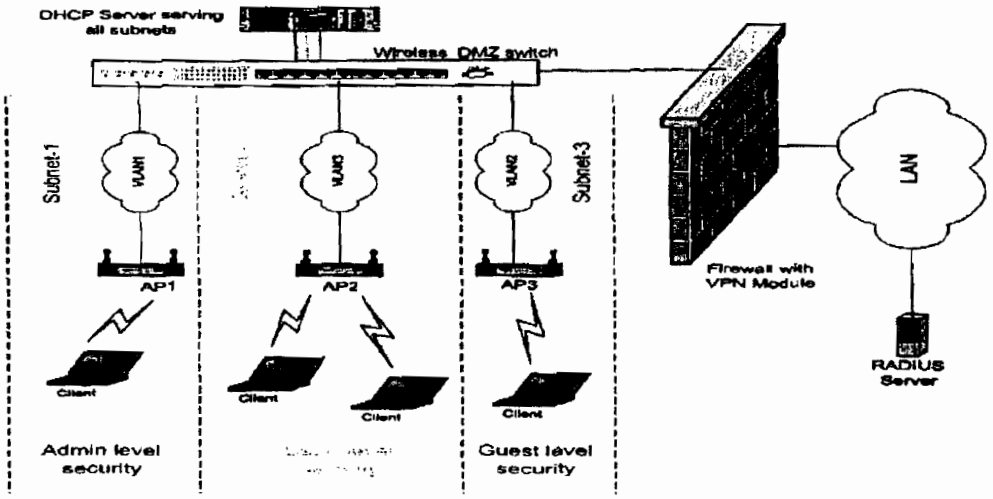



**Figure 2.25: Layered Security Approach (Erten, & Tomur, 2004).**

According to Erten and Tomur (2004) in an organization, there are various categories of users who are in need of having access to several network resources. For example, by connecting their mobile computing devices to wireless LAN, system administrators might demand access to all resources in corporate LAN with full privilege whereas other staff might only need to reach e-mail and file server for checking their corporate e-mails and accessing their home folders. Likewise, wireless Internet access might be provided for guests who possess laptops, PDA's with suitable hardware. In order to deliver sufficient security for each of these connections from wireless network to corporate LAN while not forgoing network performance, diverse levels of security actions should be put in place for different access types. Whereas, it is suitable to use certificate based authentication with strong encryption for system administrators, for instance no encryption and authentication is necessary for Internet connection of guests.

Additionally, wireless region restrictions from which precise resources on corporate network can be reached is very significant for avoidance of mischievous access, for instance permitting wireless connections to corporate LAN from the hall where coverage is delivered

only for guests; internet access might result in security breaks. The security approach depicted in figure 2.25 provides the solution for organizational networks with security requirements as pronounced in earlier paragraphs for a wireless LAN positioning. In this architecture, the security level (strength of authentication, encryption, and access rights) is achieved by the rights of the client (administrator, domain user or guest) and the place of the access points that aids the connection. In addition, when a user attempts to access a resource in corporate LAN from a location covered by wireless LAN, he or she will first be authenticated and encryption method is selected according to higher profile, then he or she is granted a suitable access level based on the location.

### 2.7.3 Layered Defense Approach to Network Security

A layered defense according to Nortel (2007) uses many approaches to security implementation at several areas within a network, where the approach eliminates single points of security failure in order to secure enterprise information assets. Serious security measures must be put in place in organization to improve their organizational effectiveness in terms of performances and reduction in security breaches (Fitzgerald, & Dennis, 1993).

As stated by Nortel (2007) merely a single virus, such as the My Doom Email virus, is estimated to have cost enterprises $22.6B, these costs don't fully reflect the damages and negative influence that organizations that have been attacked normally go through (Nortel, 2007). There is an increasing trend in sophisticated viruses, worms with payload which has to do with Trojan Horses that lie dormant and used by hackers in today's internet world. The speed at which attackers get to discover vulnerabilities in wireless networks is rapidly increasing, where several opportunities for threats come from new applications on networks,

basically, given an increase in public "Instant Messaging and Peer to Peer Networks" for file sharing. The victim machines used in launching attacks and the speed rate at which they are spread must be of great concern to organization when deploying security architecture in their environment (Nortel, 2007). Presently, Enterprises and governments are reaping the benefits of increased communications with fewer boundaries between them and their business partners, customers and distant employees. Though there are many advantages, they are as well surrounded by various risks and attacks of doing business on public or private networks, consequence to this organization must ensure that they make the right security decisions in the protection of their digital assets, such as their customer's privacy, considering the increasing business on public networks and the mobility of their employees, they are unfortunately more likely presently than ever to be victims of worms, viruses, denial of service attacks, and online fraud or theft. A mixture of creating and applying security policies that address the technical, business and human aspects of security, selecting the right security solutions and placing the suitable processes in place will assist organizations stand these challenges openly (Nortel, 2007). Eventually, a strong architecture to network security not only aid security of your network, but your general network consistency, business steadiness and business productivity.

To be able to achieve the above listed goals a Layered Defense Approach to Network Security should be adopted by organization to ensure that all single points of security failures are removed by fully leveraging the several different point security solutions, filtering systems, and observing strategies to secure information technology resources and data (Farouzan, & Fegan, 2007). However, the layered defense to network security approach according to Nortel (2007) centers on preserving proper security measures and procedures at five different levels within your wireless network environment, and they include:

(I) **Endpoint Security** for ensuring legal and valid identity of connected device in compliance with security policy.

(II) **Secure Communication** for ensuring effective information defense from unauthorized detection over the network.

(III) **Perimeter Security** for permitting the good contents in and avoiding the bad contents from having access into the network by securing the boundaries between regions of different levels of trust.

(IV) **Core Network Security** for monitoring the cruel software and traffic irregularities, applying network policy and aiding network continuity.

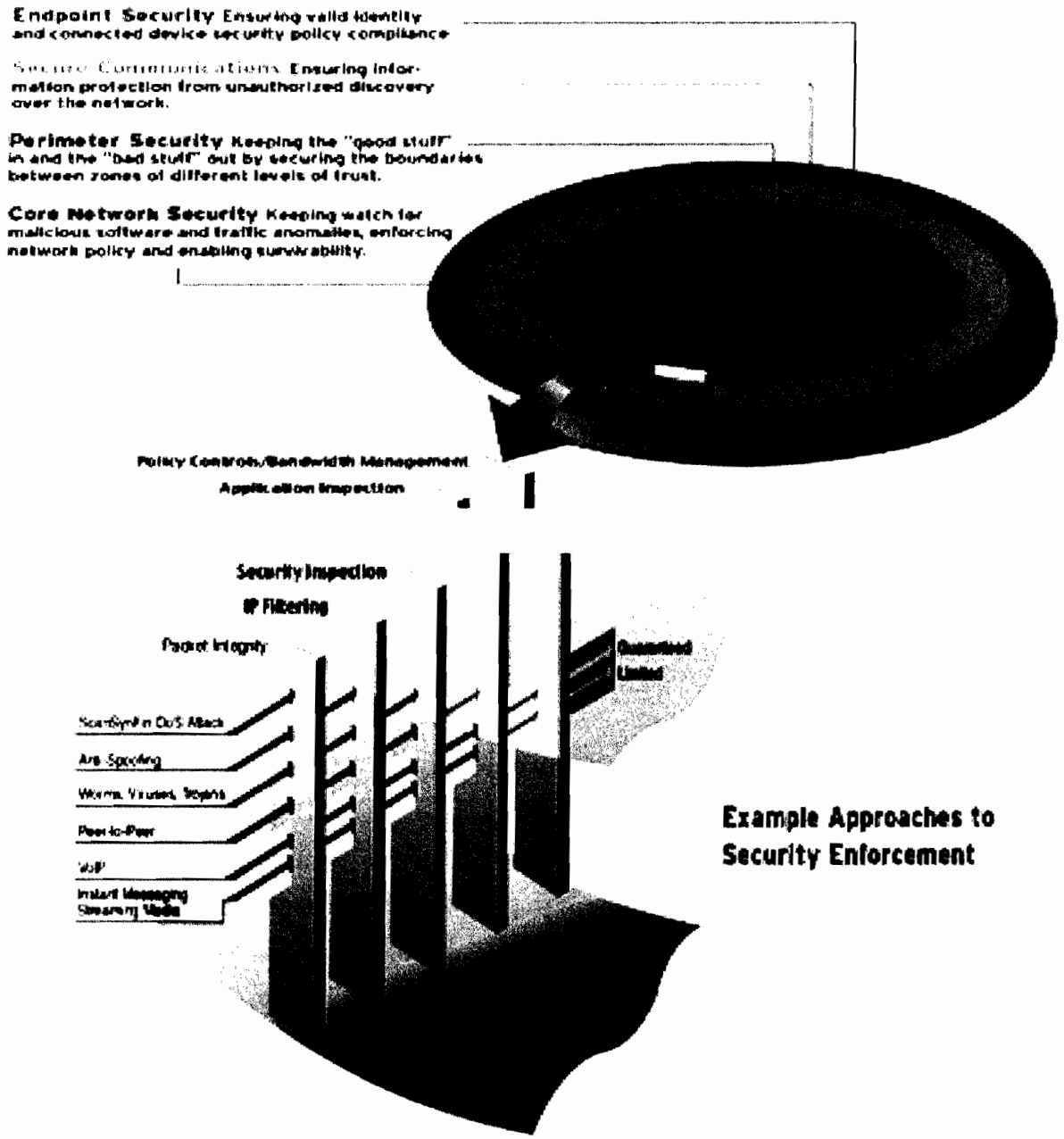



**Figure 2.26: Layered Defense Network Security Approach (Nortel, 2007).**

The above security approach in figure 2.2.7 was designed to guarantee that there are no single points of security failure in a network, by deploying security solutions at distant endpoints, mobile devices, and network and domain perimeter down to the core network. This can be achieved by deploying numerous approaches such as filters for signatures and keywords for

common attacks, encryption, firewall inspection of known protocols, anti-virus and intrusion detection and protection software for security implementation at several areas within a network. This approach is strengthened by leveraging open solutions that exploit security competences and products from best-of-breed security (Nortel, 2007).

## 2.8 Summary

This chapter was used to discuss the background of related studies that has to do with the threats and attacks encountered when securing wireless devices such as mobile computing using unlayered security approaches due to their weaknesses, as well as the benefits and advantages derived in securing mobile computing devices using the layered security approaches.

# CHAPTER THREE

# RESEARCH METHODOLOGY

## 3 Introduction

Research method refers to the methods and techniques that researchers make use of in conducting their researches. It is a formalized approach used in implementing the system development lifecycle (SDLC) and lays emphasis on process models as the core of the system concept (Dennis, Wixom, & Tegarden, 2010). This section will be made use of to explain the methodology of the research that was adopted from system development life cycle (Dennis, Wixom, & Tegarden, 2010).

The research methodology in this section will be made use of to present the phases of our research, which was made use of to achieve the designing and implementation of the chosen approach for securing mobile computing device as depicted in figure 3.1. However, as a result of the limited time constraint this project will only focus on the design and implementation of the Access Control (Authorization) and Authentication as a security measure to secure mobile computing under the Network Layer as shown below:


**Figure 3.1 : Access Control/User Authentication (Ashley, 2006)**

## 3.1 Research Design Methodology

According to Dennis, Wixom, and Tegarden, (2010) methodology is a systematic and formalized approach used in implementing the system development life cycle (SDLC). It facilitates and enhances project accomplishments by structuring interrelated processes according to the steps or phase stated, and as such confirms that a constant method is used to achieve all the steps or phases of the entire project (Hoffer, George, & Valacich, 2002).

The system was developed with Microsoft Visual Studio using ASP.NET, and as such Microsoft SQL Server 2005 was used as Database to store and query the necessary information from the database. However, the adopted methodology for this project consist of five phases as shown in figure 3.2 that has to do with Planning, Analysis, Design, Implementation and the Evaluation phase.

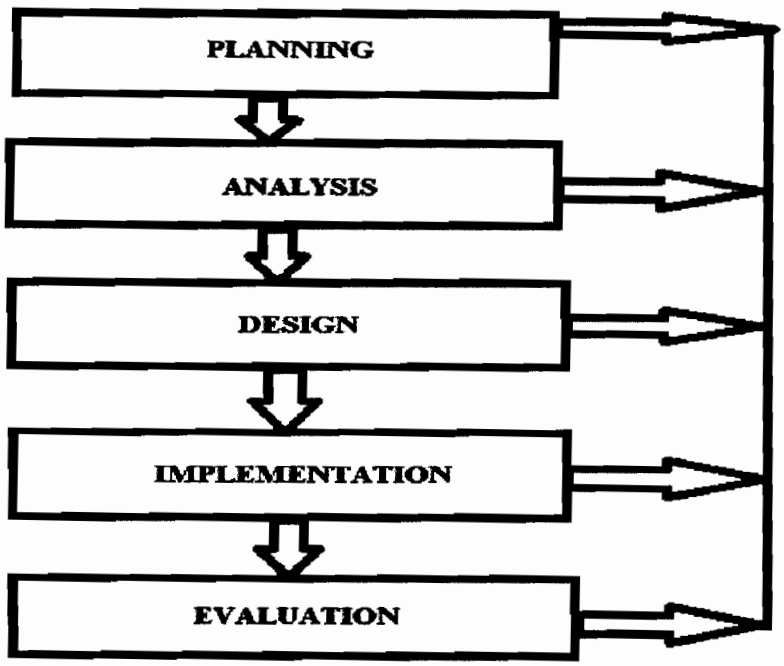



**Figure 3.2: System Development Life Cycle (Dennis, Wixom, & Tegarden, 2010)**

### 3.1.1 Planning

The planning phase is a important process of understanding why the system should be built or developed and determining how to go about in developing the system (Dennis, Wixom, & Tegarden, 2010).

### 3.1.2 Analysis

This is the phase that answers the question of who the system is actually designed for, such as who will use the system, what the system will do, and when will the system be used (Dennis, Wixom, & Tegarden, 2010). This is the phase where the current system is being investigated in order to identify improvement opportunities, and basically to develop a new concept for the new system (Dennis, Wixom, & Tegarden, 2010).

### 3.1.3 Design

This is the phase that is used to describe how the system will function in terms of the hardware, software, and network infrastructures that will be put in place, the user interface, forms and reports that will be used and the specific programs, databases and files that will be needed (Dennis, Wixom, & Tegarden, 2010).

### 3.1.4 Implementation

This is the phase during which the system is actually built and developed. It seems to be the phase that usually gets the most attention in as much as is the most longest and expensive aspect of the development process (Dennis, Wixom, & Tegarden, 2010).

### 3.1.5 Evaluation

This is the phase during which the system is systematically assessed to determine the merit and worth of the system. It is that phase where a systematic acquisition and assessment of information is been provided basically to ascertain a useful feedback about the system that was developed (Dennis, Wixom, & Tegarden, 2010).

## 3.2 Summary

This chapter was used to explain the methodology adopted in the research. Consequently, the methodology was used to standardize the approaches to be taken in the development and evaluation of the system and was adopted from System Development Life Cycle (SDLC) (Dennis, Wixom, & Tegarden, 2010) and consisted of five interrelated phases in likes of Planning, Analysis, Design, Implementation and Evaluation to be followed during the development of the system.

# CHAPTER FOUR

# ANALYSIS AND DESIGN

## 4 Introduction

This chapter entails the analysis, design and implementation, and evaluation of the Security measures for mobile computing as regard Authentication and Access Control (Authorization) for the Users, which happens to be one of the measures to be taken during the implementation of Layered Security Approach for Mobile Computing which will encompass the use of UML diagrams in likes of use case diagram, sequence diagram, as well as the interfaces of the system.

Unified Modeling Language (UML) will be made use of in designing the Use case and Sequence Diagram basically to ascertain the most important roles of the Security measures for mobile computing as regard Authentication and Access Control (Authorization) on the part of the users.

## 4.1 Use Case Model

Use case is a methodology deployed when analyzing a system basically to identify, clarify, classify, arrange and organize system requirements (Quality.com, 2009).

During analysis, analysts use class diagrams and interaction diagrams (Sequence diagram) to capture the basic understanding of the dynamic aspects of the underlying business processes. The Use Case Model is normally used to describe the functions and capabilities that a system

must deliver to its users. It also assists in defining those events that will take place inside the system. The roles that users play are usually represented using actors, and as such what the users are expected to do with the system is usually represented using the use cases. A complete course of events in the system seen from the user's perspectives can be done using use cases (Simon et al, 2005).

### 4.1.1 Use Case Diagram

Use case diagrams consist of named pieces of functionality such as use cases as well as those things invoking the functionality such as actors, and perhaps those elements in charge of implementing the use cases known as subjects. Use cases diagram can be used to capture the way system functions using Unified Modeling Language (UML).

Depicted in figure 4.1 is the User Authentication/Access Control UML Use Case Diagram concerning one of the security measures deployed under the Network layer security level under the layered security approach. The use case contains users that are expected to be granted or denied access to the network. The use case comprised of Login Authentication and Access Control/Authorization

Concerning this system, to enhance effective security measures for mobile computing users, they will have to Authenticate themselves or login using their user name and password, on the other hand, the system need to be rest assure that their username and password conforms with what have be programmed in the system before they can be granted access or authorization into the network.

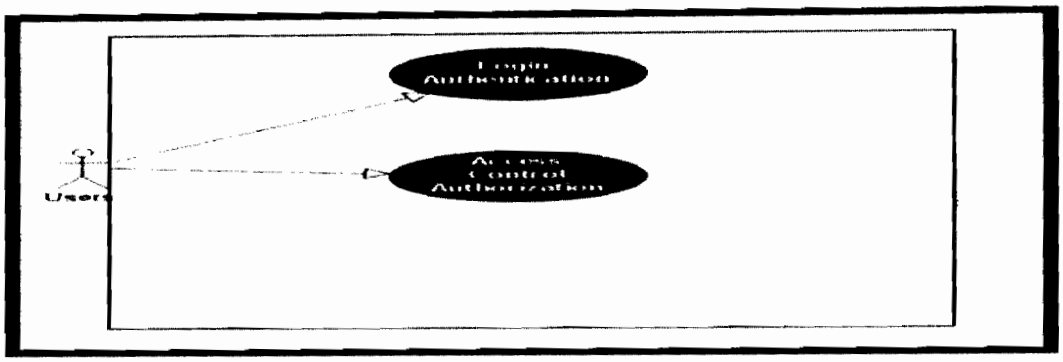


**Figure 4.1: User Authentication and Access Control UML Use Case Diagram**

### 4.1.2 Sequence Diagram for the flow of Use Cases

A sequence diagram is a dynamic model that shows the explicit sequence of messages that are passed between objects in a defined interaction (Dennis, Wixom, & Tegarden, 2010).

As depicted in figure 4.2 is the sequence diagram representing the events and processes of users when granted authorization into the wireless network zone. The process consists of login/authentication, user, controller, and entity user information page. Both actors uses their user name and password to login into the system network, where the process involves verification of user name and password verification basically to confirm if he or she can be given an authorization to come into the system network.

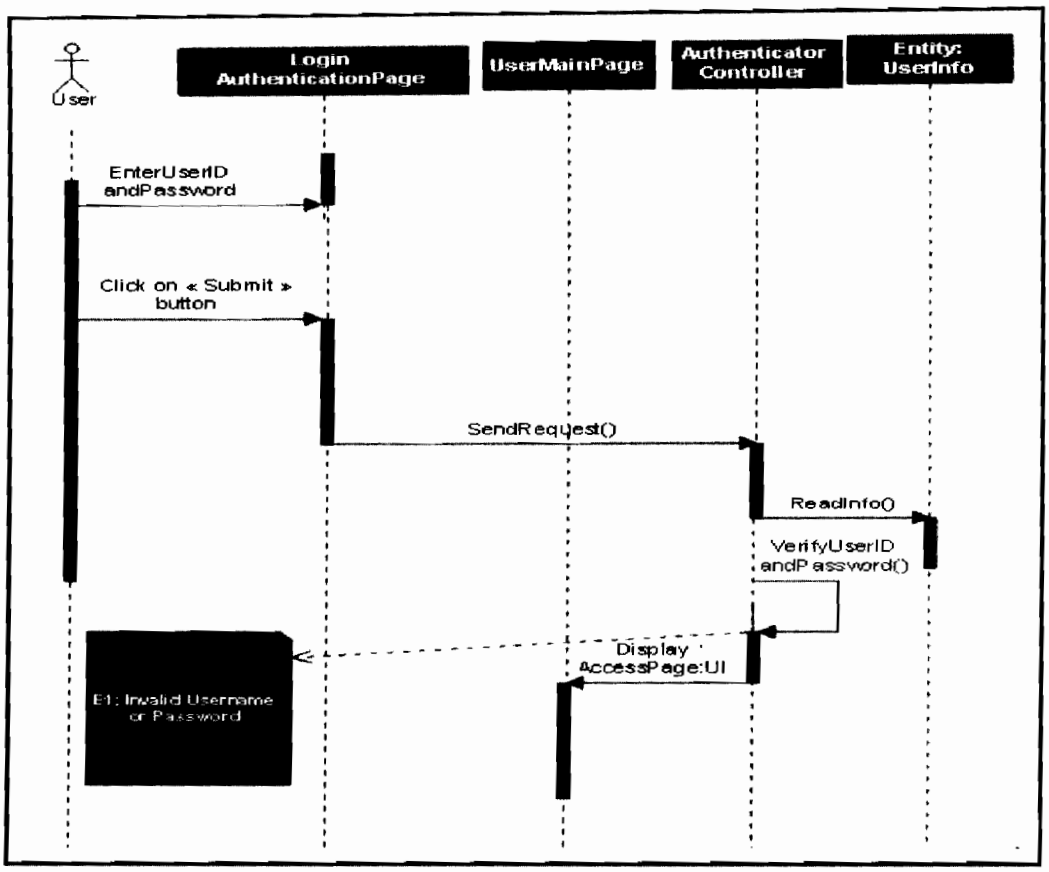



**Figure 4.2: Sequence Diagram for Use Cases Login Authentication and Access Control**

## 4.2 System Design and Development

This section comenced with the design of the of the Network after understanding why the system should be built and what actually the system ought to do.

NetBeans IDE 6.8 (Java) was made use of to design and develop security measures concerning User Authentication and Authorization to safeguard and secure mobile users from gaining free access into the network if they are not one of the valid users of that network.

Table 4.1 depicts the Integrated Development Environment of software used for the Network development.

**Table 4.1: Development environment**

| Development Environment | Applications |
|---|---|
| Programming language | Java Net beans |
| Operating System | Windows XP &Windows 7 |
| Computer Browser | Internet Explorer 7 & Google Chrome |

## 4.3 Findings and Design Interfaces

User Authentication and Access Control (Authorization) to the Network has different pages (Interfaces) done by the programmer in order to deploy strict security measures concerning User Authentication and Access Control. Interfaces are computers, appliances. Machines, mobile communication devices, software applications and websites design with the focus on the users experience and interaction, and as such, the goal of the user interface design is to enable the user's interaction with the system as simple and efficient as possible in terms of accomplishing the goals of the system (Dennis, Wixom, & Tegarden, 2010). The following interfaces were discussed below:

### 4.3.1 Mobile User Device Page

As depicted in Figure 4.3 the Mobile User Device Page, which contains the users operating system in likes of the Recycle Bin, My computer and Internet Explorer with which the mobile user can click on to gain access to the network if the network can be by pass without authenticating and being granted an access control into the network.

**Figure 4.3: Mobile User device Page**

### 4.3.2 User Authentication/Login Page

As depicted in figure 4.3 the Mobile User must insert the correct username and password to be able to authenticate him or herself, should the user inserted a wrong username or password the he or she will not be given or granted access to the network and as such the system will display Access Denied due to wrong username or password being inputted into the system by the user as depicted in figure 4.4

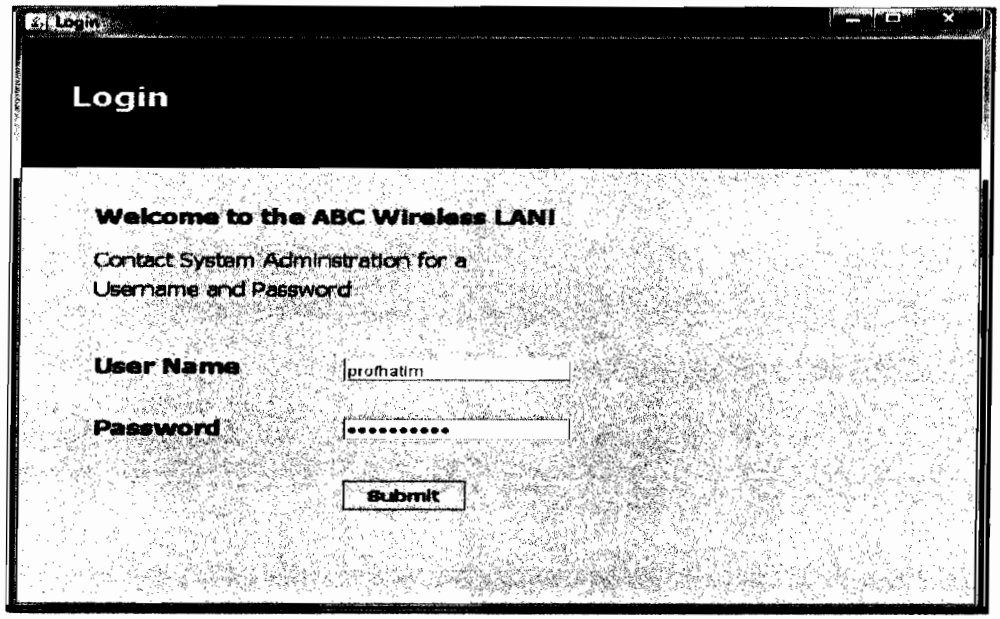



**Figure 4.4: User Login/Authentication Page**

### 4.3.3 User Access Page

As depicted in figure 4.5 if the user is a valid user of the network he or she will be able to have access to the network due to the fact that he or she will be able to provide the correct username and password given to him or her to be able to have access to the network browser.

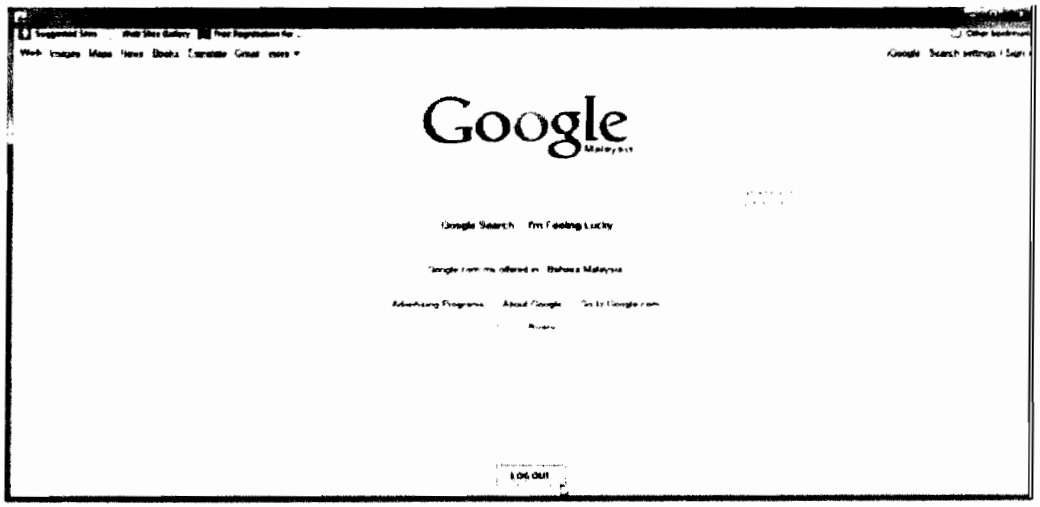



**Figure 4.5: User Access Page**

### 4.3.4 User Access Denied Page

As shown in figure 4.6 if the user is not a valid user of the network and seems to be an intruder to the network he or she will find it difficult to by pass the network due to lack of authenticating him or herself before gaining access or authorization to the network facilities.

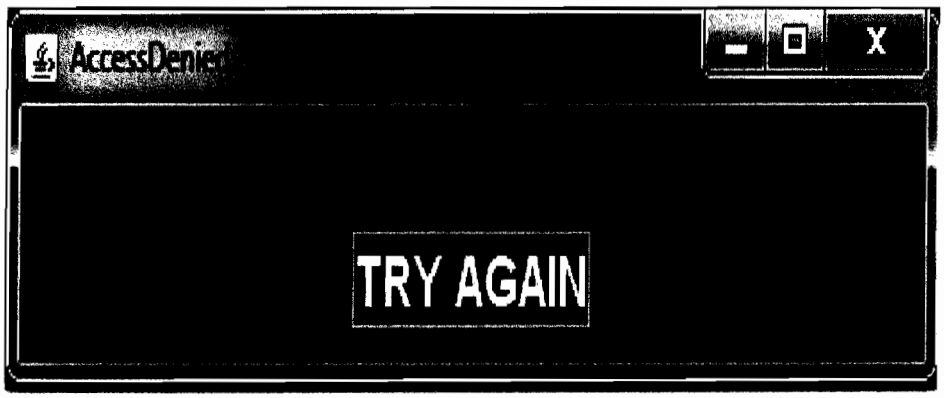



**Figure 4.6: User Access Denied Page**

## 4.4 Implementation and Evaluation

The system was implemented and evaluated by inserting valid username and password to guarantee the effectiveness of the system.

## 4.5 Summary

This chapter was used to highlight the design and development of the network concerning User Authentication and Access Control (Authorization). Consequently, the section was made use of to explain use case diagram and sequence diagram concerning the system. Nevertheless, Java Net beans programming language was used to design and develop the system. Implementation and Evaluation (Testing) was done using username and password basically to verify the originality and effectiveness of the system. In brevity, it indicates that the output and goal of the security measures concerning network layer/level under the layered security approach was able to address and fulfill the purpose of its development.

# CHAPTER FIVE

# DISCUSSION AND CONCLUSION

## 5 Introduction

This chapter discusses the findings of the study by cutting, summarizing and reviewing the findings in line with the objectives of the study, its problems and limitations as well as presenting its contribution to knowledge. Consequently, the study also suggests future studies by improving on the system such as linking it via the internet, as well as deploying other security measures stated in the layered security approach.

## 5.1 Discussion

As stated in the earlier section of this study, the aim of this study is to develop an Authentication and Access Control Security system which happens to be one of the steps involved in securing mobile computing devices as regard layered security approach. However, by doing this will assist the organization to safeguard and protect their network from unauthorized access to their facilities. The system was developed using Java NetBeans IDE 6.8, Windows XP and Windows 7, Internet Explorer and Google Chrome. The methodology for the system development used in this research was adopted from System Development Lifecycle (SDLC) which comprises of five phases such as System Planning, Analysis, Design, Implementation and Evaluation.

## 5.2 Study Limitation

(I) One of the limitations of this study is that the system was tested using local host server such as Java Net beans. However, due to the limited time coupled with financial constraints, no access points or web server was employed in testing the system.

(II) A small number of preceding studies (Layered Security Approach for Mobile Computing) were obtainable and as such hold back the study in having adequate resources on related research work except papers on general and organization internet security approaches.

## 5.3 Contribution of the Study

Mobile Computing devices should be deployed and used by organization as a result of its features and capabilities such as an operating range of up to 150 feet indoors and 1500 feet outdoors, and can also speed like the Ethernet technologies without wires, and can transfer 54Mbits per second which is significantly faster than the original Ethernet. Though, the rise of the internet with prospects of using mobile computers anywhere in the world has dramatically amplified the probable vulnerability of organizations digital assets against so many security threats, consequence to this magnitude on network security need to be put into consideration as a result of the severe undefended security break in, and should be noted that any possible losses related with security failures of organizations relating to their wireless network for just 24 hours can cost organization $1 million.

Nevertheless, upon the deployment and implementation of the security measures concerning layered security approach for mobile computing will enable organizations digital asset to be protected and safeguarded from hackers and other cyber terrorists that are launching network attacks with increasing frequencies and sophistication. Consequently, the security measure deployed in this study will restrict hackers from coming into the network in order for the network to be fully secured from any unauthorized access to the network, and as such by selectively deploying security measures using a layered approach within network environment will adequately protect and secure organizations digital assets and greatly reduce their exposure to most network blemishes and breaches.

## 5.4 Recommendation for Future Research

Layered security approach enables organizations digital asset to be adequately protected and secured against any possible attacks from unauthorized users. This study suggests areas for future studies to expand on this research concerning the scope of the research as a result of its limitations relating to only the network layered that dealt with only on the Authentication and Access Control security measures thus, further security deployments have to be done concerning other security levels as well as putting into consideration their security measures.

Nonetheless, this study will provide future channel for students, researchers and organizations that intend working on related subject matter as well as its development.

## 5.5 Conclusion

Layered security approach for the restrictions of mobile computing users to network facilities was developed to assist in securing organizations digital assets. The system was evaluated and the results confirm that it is useful for organizations using wireless network resources basically to safeguard and protect their network against cyber terrorists, attackers and hackers from having access to their network facilities.

In other words, it is hoped that the findings of this research will motivate and encourage organizations to incorporate and deploy layered security approach in improving and enhancing their network security against any possible attacks from external users.

# REFERENCE


Agarwal, A, K., Wang, W., & McNair, J, Y. (2005). An Experimental Study of Cross-Layer Security Protocols in Public Access Wireless Networks: In proceedings of IEEE/GLOBECOM, pp. 1747-1751.

Agrawal, P., & Famolari, D. (1999). Mobile Computing in Next Generation Wireless Networks.

Amor (2002). Internet future Strategies: How pervasive computing services will change the world. USA: Prentice Hall.

Arbaugh, W. A., Shankar, N., and Wan, J. (2002). Your 802.1 I network has no clothes. IEEE Wireless Communications.

Ashley, M. (2006). Layered Network Security: A Best Practices Approach: In proceedings of CTO and VP of Customer Experience StillSecure.

Avancha, S. (2005). A Holistic Approach to Secure Sensor Networks PhD Dissertation University of Maryland.

Baghaei, N., & Hunt, R. (2004). IEEE 802.11 Wireless LAN Security Performance using Multiple Clients, Associate Professor, Department of Computer Science and Software Engineering University of Canterbury.

Baghaei, N., & Hunt, R. (2004). IEEE 802.11 Wireless LAN Security Performance using Multiple Clients, Associate Professor, Department of Computer Science and Software Engineering University of Canterbury.

Blackert, W. J., Gregg, D. M., Castner, A.K., Kyle, E.M., Hom, R.L., & Jokerst, R.M. (2003). Analyzing interaction between distributed denial of service attacks and mitigation technologies, Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24, pp. 26 – 36.

Borisov, N. Goldberg, I. & Wagner, D. (2001). Intercepting Mobile Communications: The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf.

Borisov, N., Goldberg, I., and Wagner, D. (2001). Intercepting mobile Communications: The insecurity of 802.11, In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking.

Borisov, N., Ian G., & David W. (2001). Intercepting Mobile Communications: The Insecurity of 802.11, in the Proceedings of the Seventh International Conference on Mobile Computing and Networking.

Burell, J. (2002). Wireless Local Area Networking (WLAN) Security Assessment and Countermeasures. In proceedings of IEEE, 802.11 Wireless Network.

Carey, A. (2001). Wireless Security Vulnerabilities continue to Surface: Cigital Identifies the Latest. White Paper by Cigital, Inc. http://www.cigital.com.

Carlsson, C., Carlsson, J., & Walden, P. (2005). Mobile Services For The Hospitality Industry. Paper presented at the Thirteenth European Conference on Information Systems, Regensburg, Germany.

Carlsson, C., Carlsson, J., & Walden, P. (2005). Mobile Services For The Hospitality Industry. Paper presented at the Thirteenth European Conference on Information Systems, Regensburg, Germany.

Cheng, J. (2008). Testing and Debugging Persistent Computing Systems: A New Challenge in Ubiquitous Computing. In proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 408-414.

Cisco Systems. "Cisco Security Advisory (2001/2002): Catalyst 5000 Series 802.1x Vulnerability. URL: http://www.cisco.com/warp/public/707/cat5k-8021x-vuln-pub.shtml.

Cisco Validated Design, (2008). Wireless and Network Security Integration Design Guide: Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883.

Cole, E. (2002). Hackers Beware. Boston, MA: New Riders.

Colubris Networks, Inc (2002). Comparing Colubris IPSEC Wireless Access Point Solutions with Cisco Safe for Wireless LANs. 2002 Webpage online available at http://download.colubris.com/library/whitepapers/WP-020912-EN-01-00.pdf.

Connolly, P.J. (2002). The trouble with 802.1x." InfoWorld. 8 March 2002. URL: http://www.infoworld.com/articles/fe/xml/02/03/11/020311fe8021x.xml.

Corral, G., Cadenas, X., Zaballos, A., & Cadenas, M,T. (2005). A Distributed Vulnerability Detection System for WLANs: In proceedings of the First International Conference on Wireless Internet.

Craiger, J,P. (2002). Streamline IT security environments and compliance processes, 802.11, 802.1X, and Wireless Security.

Dankers, J., Garefalakis, T., Schaffelhofer, R., & Wright, T. (2002). Public key infrastructure in mobile systems. Electronics and Communication Engineering Journal.

Dawkins, J., & Dale, J. (2004). "A Systematic approach to Multi- Stage Network Attack Analysis", Proceedings of the 2nd. IEEE IWIA'04, 0-7695-2117-7/04, 2004.

Dennis A., Wixom B, H., & Tegarden D, (2010). System Analysis and Design with UML: Object-Oriented Approach, Third Edition. John Wiley & Sons, Inc.

Dong W. J., & Doo-Kwon B. (2002). An Adaptive Mobile Computing Model for Dynamic Resource Management in Distributed Computing Environments remarkable, Springer-Verlag Berlin Heidelberg, LNCS 2344, pp. 671-678.

Douceur, J. (2002). The Sybil Attack: 1st International Workshop on Peer-to-Peer Systems.

El-Alfy, E.-S. M. (2005). A General Look at Building Applications for Mobile Devices.

Erten, Y, M,. & Tomur, E. (2004). A Layered Security Architecture for Corporate 802.11 Wireless Networks. In proceeding of IEEE, pp.123-128.

Farouzan, B, A., & Fegan, S, C. (2007). Data Communications and Networking, TCP/IP Protocol Suite Local Area Network, Business Data Communication, forth edition, McGraw- Hill Forouzan Networking Series, Higher Education.

Fitzgerald, J., & Dennis, A. (1993). Business Data Communications and Networking: Basic Concepts, Security and Design, 4th Edition.

Fleck, B. & Jordan D., (2002). Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network. White Paper by Cigital, Inc. http://www.cigital.com.

Fluher, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. http://downloads.securityfocus.com/library/rc4_ksaproc.pdf.

Fluhrer, S., Martin, I., & Shamir, A. (2001). Weaknesses in the key scheduling algorithm of RC4, Eighth Annual Workshop on Selected Areas in Cryptography.

Geier, J. (2002)"802.11 WEP: Concepts and Vulnerability." 802.11 Planet.

Hoffer, J. A., George, J., & Valacich, J. (2002). Modern Systems Analysis and Design.
http://staging.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml.

IEEE. "IEEE 802.1x-2001 (ISO/IEC 802-1x: 2001), Part 11: Wireless LAN Medium Access Local and metropolitan area networks: Port-Based Network Access Control." URL: http://standards.ieee.org/getieee802/download/802.1X- 2001.pdf.

International Engineering Consortium (2007). Web ProForums Retrieved August 13, 2009, from http://www.iec.org/online/tutorials/wap/index.html.

Ivan K. (1998). Software Vulnerability Analysis, Ph.D. thesis, Department of Computer Sciences, Purdue University, https://www.cerias.purdue.edu/techreports-ssl/public/98-09.pdf.

Kalkbrenner, G., & Nebojsa, F. (2001). Campus Mobil: Mobile Services for Campus and Student needs Retrieved August 15, 2009.

Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., & Frantzen, M. (2001). Analysis of Vulnerabilities in Internet Firewalls: Center for Education and Research in Information Assurance and Security (CERIAS).

Karygiannis & Owens, (2002). Wireless Network Security 802.11, Bluetooth and Handheld Devices. Recommendations of National Institute of Standards and Technology, on Wireless Network Security, pp. 1-119.

Koudounas & Iqbal, (1996). Mobile computing: past, present and future.

Koudonnas, V., & Iqbal, O. (1991). Mobile computing: past, present and future. N. Sollenberger, N. Seshadri, and R. Cox, "The Evolution of IS-136 TDMA for Third Generation Wireless Services", IEEE Personal Communications, Vol. 6, No. 3.

Krishnamurthy, Prashnt, Joseph Kabara, Tanapat Anusas-amornkul. (2002). Security in Wireless Residential Networks, IEEE Transactions on Consumer Electronics, Vol 48, No 1, pp 157- 166.

Kurose, J, F., & Ross, K, W. (2008). Computer Networking A Top-Down Approach, fourth edition, Pearson International Education.Inc.

Kustin, S. (2002). The Proliferation of Wireless Internet Access Devices and its Effect on Consumer Behavior Patterns.

Lockhart, A. (2006). Network Security Hacks Second Edition.

Loeb, L. (2002). What's up with WEP? http://www.106.ibm.com/developerworks/library/s-wep/.

Lynn, M., & Robert B. (2002). Advanced 802.11 Attack, presentation to Black Hat Conference, Las Vegas, NV 31 July 2002. Available at http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt.

Bishop, M., & Bailey, D. (1996). A critical analysis of vulnerability taxonomies," in Proceedings of the NIST Invitational Workshop on Vulnerabilities, July 1996, Also appears as Technical Report 96-11, Department of Computer Science, University of Califonia at Davis, http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/ucd-ecs-96-11.ps. Also see Classifying Vulnerabilities, A Taxonomy of UNIX and Network Security Vulnerabilities, as well as Vulnerabilities Analysis by same author.

Mishra, A., & Arbaugh, W. (2002). An initial security analysis of the 802.1x standard. http://www.cs.umd.edu/~waa/1x.pdf.

Mishra, A., & William, A. (2002). An Initial Security Analysis of The IEE 802.1X Standard. University of Maryland, Department of Computer Science and University of Maryland Institute for Advanced Computer Studies Techniacal Report CS-TR-4328 and UMIACS-TR-2002-10 6.

Moioli, F. (2000). Security in Public Access Wireless LAN Networks, Masters Thesis, Department of Teleinformatics, Royal Institute of Technology, Stockholm, Sweden. New Jersey: Prentice Hall.

Newsome, J., Shi, E., Song, D, & Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, pp. 259 – 268.

Nortel (2007). Layered Defense Approach to Network Security: Nortel, the Nortel logo, Nortel Business Made Simple, the Globemark, Alteon, BayStack, Contivity, Passport and Optivity are trademarks of Nortel Networks.

Nylander, S. (2004). Different Approaches to Achieving Device Independent Services an Overview: Swedish Institute of Computer Science.

Open Mobile Alliance (OMA) (2004). Open Mobile Alliance Overview Retrieved August 13, 2009,
from http://www.openmobilealliance.org/docs/OMAShortPaper_May2004v.1.pdf.

Pathan, A, K., Lee, H., W., & Hong, C, (2006). Security in Wireless Sensor Networks: Issues and Challenges. In proceedings of IEEE 8th International Conference. On Advanced Communication Technology, pp. 6-1048.

Pullen, M. (2000). The Internet Protocol Stack and the Network Workbench, Through Hands-On Programming, pp. 1-10.

Roshan, P. (2001). 802.1X authenticates 802.11 wireless." NetworkWorldFusion.URL: http://www.nwfusion.com/news/tech/2001/0924tech.html.

Quality.com (2009): Definition of Use Case. Retrieved August 25, 2009 from

http://searchsoftwarequality.techtarget.com/defination/

Schei, E., & Fritzner, T. C. (2002). MOWAHS: A Study of Applications for Mobile Work.

Schwartz, E. (2002). Researchers crack new wireless security spec." InfoWorld. 14 February 2002,
URL: http://www.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml. (12 June 2002).

Schwartz, E. (2002). Researcher crack new wireless security spec. InfoWorld.

Shuyao, Y., Youkun, Z., Chuck, S., & Kai, C. (2004). A security architecture for Mobile Ad Hoc Networks. Institute of Computer Technology, School of Software, Computer Network Information Bell Labs Computer Network, Center of Chinese Academy of Sciences,pp. 1-4.

Simon et al, (2005).Object-Oriented Systems Analysis and Design: Using UML. US, Third

edition, pp 230.

Simoneau, P. (2006). The OSI Model: Understanding the Seven Layers of Computer Networks. Global Knowledge Global Knowledge Training LLC, pp. 1-11.

Skoudis, E. (2002). Counter Hack: A Step-by-Step Guide t Computer Attacks and Effective Defenses. Prentice Hall, Upper Saddle River, New Jersey. pp 351-358.

Sung-Hoon, P. (2003). AN Efficient Election Protocol in Mobile Computing Environment", Springer-Verlag, Berlin Heidelberg, LNCS 2657, pp. 387-396.

Surman, G. (2002). Understanding Security Using the OSI Model, SANS Institute Information Security Reading Room. Assignment Version: GSEC Practical Version 1, pp. 1-20.

Tillwick., H, & Olivier., M. S (2004). A layered security architecture, in Proceedings of the Fourth Annual Information Security South Africa Conference, Midrand, South Africa.

Turban, E., Leidner, D., McLean, E., & Wetherbe, J. (2007). Information Technology for Management: Transforming Organizations in the Digital Economy (6th ed.): John Wiley & Sons.

Turisco, F., & Case, J. (2001). First Consulting Groups, Wireless and Mobile Computing, prepared for California Healthcare Foundation.

Walker, J., & Gmup, E. (2000). Unsafe at any key size: An analysis of the WEP encapsulation, IEEE 802.11 Task.

Wang, B.T., & Schulzrinne, H. (2004). An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2, pp. 901 – 904.

WapForum (2002a). What is WAP Retrieved July 20, 2009, from http://www.wapforum.org/faqs/index.htm.

Wapforum (2002b). Wireless Application Protocol (WAP 2.0): Technical White Paper Retrieved from www.wapforum.org/what/WAPWhite_Paper1.pdf.

Welch, D., & Lathrop, S. (2003). Wireless Security Threat Taxonomy. In proceedings of IEEE Systems, on Man and Cybernetics Society, Information Assurance Workshop, 76-83.

Wenliang Du., & Aditya P. M. (1998). Categorization of software errors that led to security breaches," in Proceedings of the 21st National Information Systems Security Conference , http://www.cerias.purdue.edu/homes/duw/research/paper/nissc98.ps.

Wenliang Du., & Aditya P. M. (2000). Testing for software vulnerability using environment perturbation, in Proceeding of the International Conference on Dependable Systems and Networks (DSN 2000), Workshop On Dependability Versus Malicious Faults, pp. 603–612,http://www.cerias.purdue.edu/homes/duw/research/paper/ftcs30 workshop.ps.

Whalen, S. (2002). An Introduction to Arp Spoofing, April 2001 webpage online available at http://packetstormsecurity.nl/papers/protocols/intro_to_arp_spoofing.pdf last accessed.

Xi Wang, Xu Liu, Xiaoge Wang & Yu Chen. (2004). A Middleware Based Mobile Scientific Computing System- MobileLab" , Springer-Verlag Berlin Heidelberg, LNCS 3251, pp. 1013-1016.

Yang, H., Xie, L., & Sun, J. (2004). Intrusion detection for Wireless Local Area Network. In proceeding of IEEE Canadian Conference on Electrical and Computer Engineering, 4, 1949-1952.

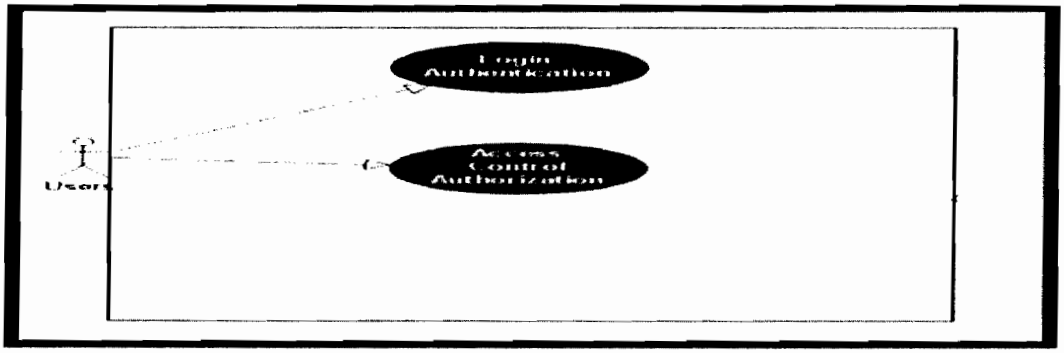
Zhiming, Q., & Jingmei, W. (2009). Application of primary components analysis of security threat in wireless network. Journal of ISECS International Colloquium on Computing, Communication, Control, and Management.

APPENDIX

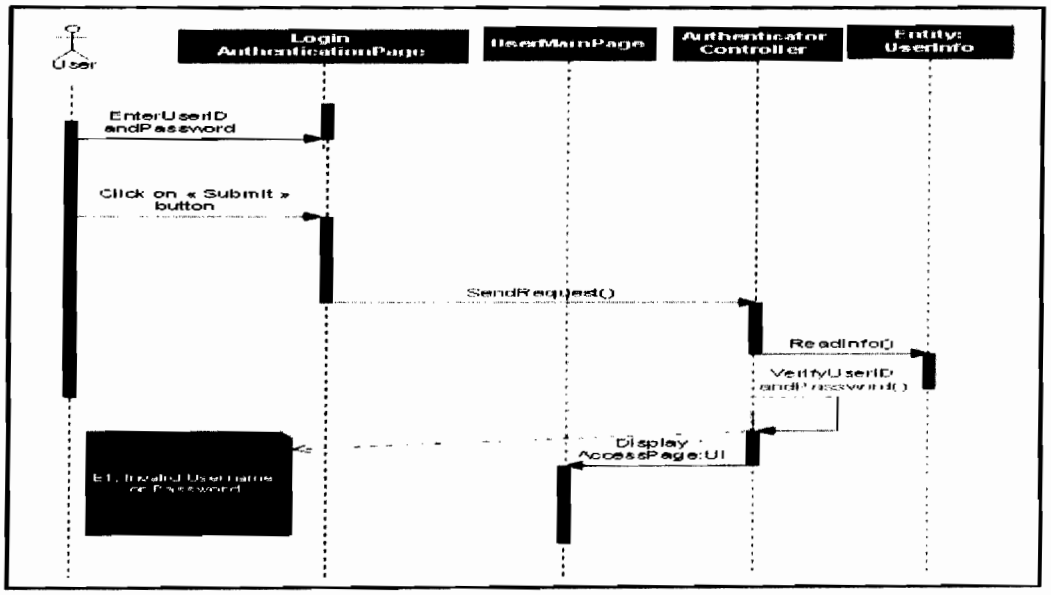
Layered Security Approach for Mobile Computing

**Analysis and Design Systematic Diagram:**

Use Case Diagram:




Sequence Diagram:



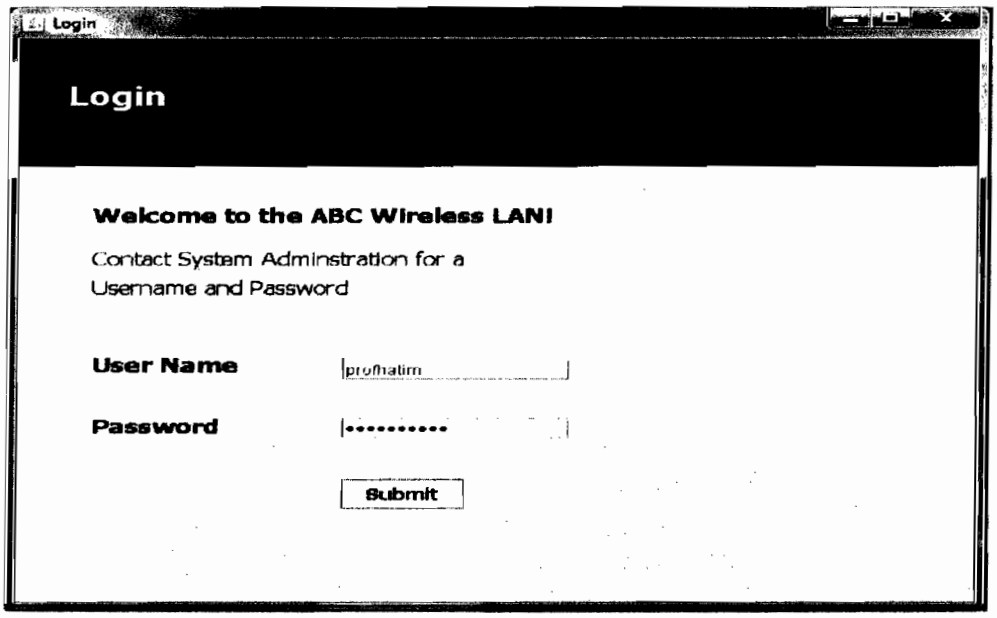
System Design and Development:

| Development Environment | Applications |
|---|---|
| Programming language | Java Net beans |
| Operating System | Windows XP &Windows 7 |
| Computer Browser | Internet Explorer 7 & Google Chrome |

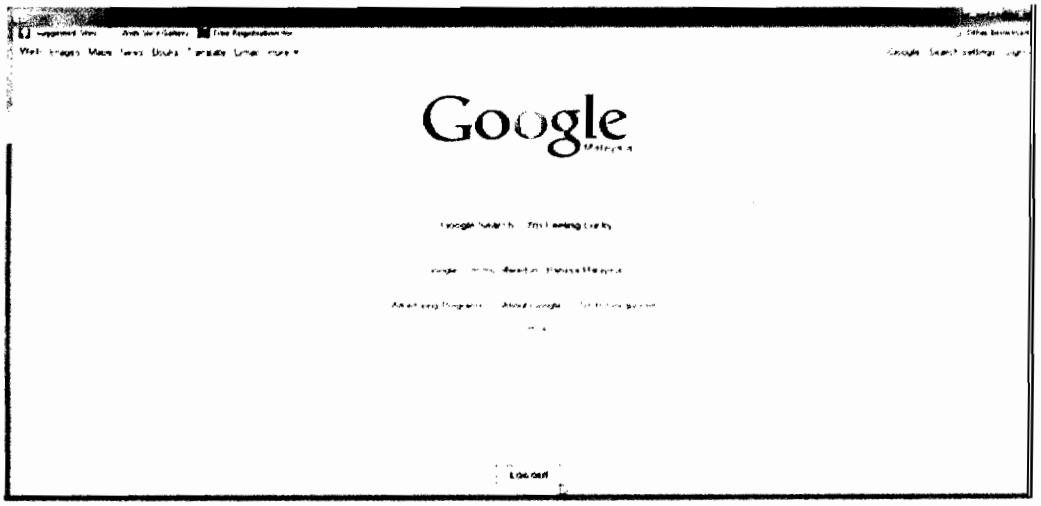
**Design Interfaces:**

Mobile User device Page:

User Authentication Page




**User Access Page**



**User Access Denied Page**