MEE09:47

Security Issues in Wireless Systems

NASEER AHMAD (740302-P210)

This thesis is presented as part of the Degree of Masters in Electrical Engineering with emphasis on Telecommunications

Blekinge Institute of Technology

July 2009

Blekinge Institute of Technology
School of Computing
Supervisor: Markus Fiedler
Examiner: Markus Fiedler

Master's Thesis MEE09:47
Department of Computing
Blekinge Institute of Technology

Master's Thesis MEE09:47
Department of Computing
Blekinge Institute of Technology

ABSTRACT

Wireless Communication is one of the fields of Telecommunications which is growing with the tremendous speed. With the passage of time wireless communication devices are becoming more and more common. It is not only the technology of business but now people are using it to perform their daily tasks, be it for calling, shopping, checking their emails or transfer their money.

Wireless communication devices include cellular phones, cordless phones and satellite phones, smart phones like Personal Digital Assistants (PDA), two way pagers, and lots of their devices are on their way to improve this wireless world. In order to establish two way communications, a wireless link may be using radio waves or Infrared light. The Wireless communication technologies have become increasingly popular in our everyday life. The hand held devices like Personal Digital Assistants (PDA) allow the users to access calendars, mails, addresses, phone number lists and the internet. Personal digital assistants (PDA) and smart phones can store large amounts of data and connect to a broad spectrum of networks, making them as important and sensitive computing platforms as laptop PCs when it comes to an organization's security plan. Today's mobile devices offer many benefits to enterprises. Mobile phones, hand held computers and other wireless systems are becoming a tempting target for virus writers. Mobile devices are the new frontier for viruses, spam and other potential security threats. Most viruses, Trojans and worms have already been created that exploit vulnerabilities. With an increasing amount of information being sent through wireless channels, new threats are opening up. Viruses have been growing fast as handsets increasingly resemble small computers that connect with each other and the internet. Hackers have also discovered that many corporate wireless local area networks (WLAN) in major cities were not properly secured. Mobile phone operators say that it is only a matter of time before the wireless world is hit by the same sorts of viruses and worms that attack computer software.

Master’s Thesis MEE09:47
Department of Computing
Blekinge Institute of Technology

ACKNOWLEDGEMENT

I would certainly like to express my gratitude to all those who gave me the possibility to complete this report. Especially Prof Markus Fiedler is the first person whose I would like to thank. During the study of Network management and during the Thesis I have known that Sir Markus Fiedler as a sympathetic and principle-centered person. His overly enthusiasm and integral view on research and his mission for providing only high quality and not less has made a deep impression on me. I am really glad that I have come to get know Markus Fiedler in my life.

SCOPE

The scope of this thesis is to look into the wireless technology as thoroughly as possible and studying the different aspects and challenges related to wireless technology which is becoming and will be the most common communication technology in the near future. We will do detailed research in finding the viable solutions to the problems faced by Wireless Communication devices and possible security measures which should be done in advance to minimize these security threats to our systems.

OBJECTIVES

The main objectives of this thesis will be:

- To study the various aspects of wireless communication technologies.
- To study the different types of wireless communication technologies.
- To study different types of wireless Communication devices.
- To study the challenges faced by wireless Communication devices in terms of security, threats and viruses.
- Suggesting implementable solutions for these security challenges.

Table of Contents

CH NO:1

1. INTRODUCTION:-

In telecommunication industry, the field of wireless communication is very rapid growing segments. In our daily life, wireless communication systems such as cordless, cellular, and satellite phones as well as wireless local area networks (WLANS) have found a widespread use and have become an essential part of their lives. This is the matter of time that the number of wireless subscribers will be higher than the number of wire line subscribers; this is mainly because of the freedom of cables which enables communication anytime, anywhere and with anyone. Now a day mobile wireless technology is emerging so rapidly that it is becoming very difficult to keep up with the latest advances in it.

Personal Digital Assistants (PDA) which is one of the hand held device make possible for its users to access calendars, emails, addresses, phone number lists and the internet also. Smart phones and Personal digital assistants (PDA) can store a large amount of data and connect to a broad spectrum of networks and makes them as important and also sensitive computing platforms as laptop PCs when it comes to an organization's security plans. As compared to the past, today's mobile devices offer many benefits to enterprises. Today mobile phone networks are rapidly adopting standard net technologies that make it easier for them to offer multimedia services. There is also disadvantage of these changes as it makes phones vulnerable to some of the infection techniques used by many desktop computer viruses also.

Aims and Description

Today's hand held computers, mobile phones, and like other wireless systems are becoming a target for virus writers. Much of the viruses, Trojans and worms which have already been created that exploit vulnerabilities. New threats are opening up with an increasing amount of information being sent through wireless channels. As handsets increasingly resemble small computers that connect with each other and the internet so Viruses have been growing fast. Many of the hackers also discovered that many of the wireless networks which are even operated by many big firms and in big cities are not secured properly. With the help of critical mass virus writers want to hit as many as people as possible. According to Mobile phone operators it is only a matter of time before the wireless world is hit by the same sorts of viruses and worms that attack computer software.

This thesis aims to analyze the threats of viruses in the wireless communication systems like Personal Digital Assistants (PDAs), Wireless Local Area Networks (WLANS)wireless wide area networks and suggestions to avoid from threats, by giving different security solutions and their importance in daily life.

1.1 THE NEED FOR ELECTROMAGNETIC SPECTRUM

Those systems which exchange information by means of a wireless channel are called the wireless communication systems.
The explanation of radio wave propagation is compulsory in order to explain the wireless transmission. The wireless transmission plays a very vital role in order to design the wireless communication systems and networks but even there are two major disadvantages of the wireless systems when compared with the wire line systems. First disadvantage is the increased bit error rate (BER) due to noise in atmosphere physical obstruction, multipath propagation and interference from other systems of communication. Second fact is that in wireless systems unlike wire line, cannot propose the exact geographical location to which signal propagation is confined resulting in the interference from the neighbouring wireless systems which are using the same waveband. In order to avoid this interference, licensing procedures were introduced in the form of Electromagnetic Spectrum.

Actually it comprises of the number of parts called bands which are used to explain the different properties of various spectrum parts. A electromagnetic spectrum consists of radio waves, micro waves, infrared, visible light, ultraviolet rays, X rays and gamma rays on the scale of frequency.

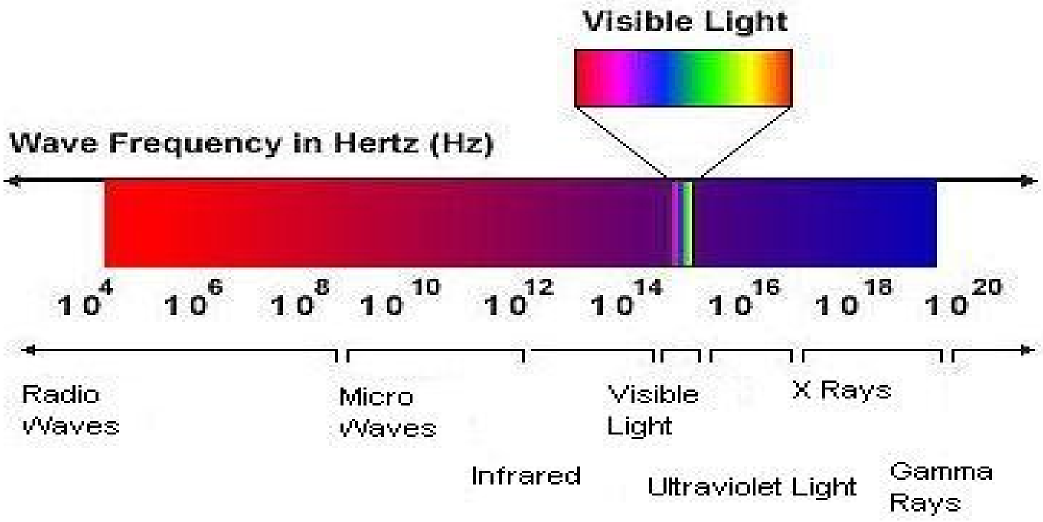


Figure 1.1 The Electromagnetic Spectrum [1]

The table below illustrates the various radio frequency bands.

Frequency	Band Name	Applications
< 3KHz	Extremely Low Frequency (ELF)	Submarine Communications
3 KHz-30 KHz	Very Low Frequency (VLF)	Marine Communications
20 KHz-300 KHz	Low Frequency (LF) or Long Wave (LW)	AM radio
300KHz-3 MHz	Medium Frequency (MF) or Medium Wave (MW)	AM radio
3 MHz-30 MHz	High Frequency (HF) or Short Wave (HW)	AM radio
30 MHz- 300 MHz	Very High Frequency (VHF)	FM Radio-TV
300 MHz-3 GHz	Ultra High Frequency (UHF)	TV-cellular telephony
3 GHz-30 GHz	Super High Frequency (SHF)	Satellites
30 GHz-300 GHz	Extra High Frequency (EHF)	Satellites-radars

Table 1.1: Various Radio Bands and their use [2]

1.2 BENEFITS OF WIRELESS TECHNOLOGY

It offers organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs also. Coverage range of wireless technologies is very broad which is very helpful for users according to their use. WLAN devices provide facility to its users to move their laptops and other handheld devices from place to place within their offices without the need for wires and without even losing network connectivity.
Basically less wiring means greater flexibility, increased efficiency, and reduced wiring costs as well .In Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between the devices.

1.3 Wireless Networks

Basically wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks. Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range. Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN).

1.3.1 Wireless LANs

WLANs provide users greater flexibility and portability than the traditional wired local area networks (LAN). In a traditional LAN, which requires a wire to connect a user’s computer to the network, a WLAN connects computers and other components to the network using an access point device which can be a wireless router only. Function of wireless access point or wireless router is that it can communicate with wireless network adaptors. Coverage range of most access point is about one hundred meters which is also called its cell or range and its users have advantage to move freely in this cell range, with their laptop or other network device. Access point cells can also be linked together to allows users to even “roam” within a building or between different buildings

1.3.2 Ad Hoc Networks

Bluetooth which is one of the Ad hoc networks are designed to dynamically connect remote devices such as cell phones, laptops, and PDAs etc. Basically these networks are termed as ad hoc because of their shifting network topologies. As the wireless lanes has a infrastructure which is fixed so Ad Hoc networks can maintain random network configurations .It also controls the flow of data between devices that are capable of supporting direct links to each other in the system.

1.4 Wireless Devices

Today a large number of devices are using wireless technologies mostly handheld devices.
The most commonly wireless handheld devices are text-messaging devices, PDAs, and smart phones.

1.4.1 Personal Digital Assistants (PDA)

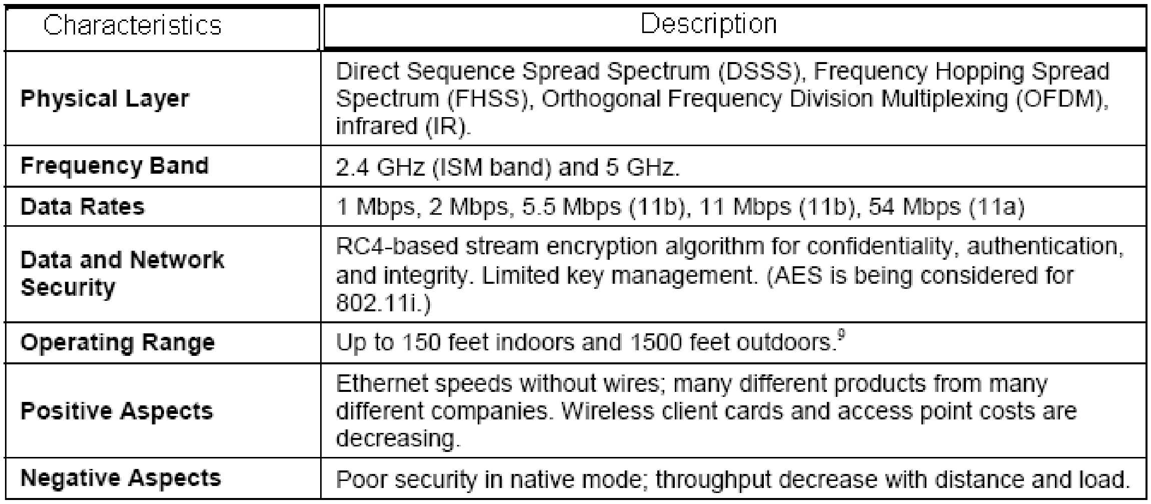
Basically PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. Personal Digital Assistants has applications like office productivity, address books and to do lists. PDAs make it possible for users that they can synchronize their data between their personal computer and PDAs or between two PDAs at the same time.
Today most of the PDAs can has their access to Internet, intranet or to the wireless wide area). New versions allow users to download their e-mail and to connect to the Internet.

1.4.2 Smart Phones

Mobile phones which have information-processing and data networking capabilities are called smart phones. Basically a Smartphone is any electronic handheld device that integrates the functionality of a cell phone, PDA or other information appliance.
Smartphone features tend to include Internet access, e-mail access, scheduling software ,built in-camera, contact management, GPS navigation software have the ability to read business documents in a variety of formats such as PDF and Microsoft office as well. Mobile wireless telephones, or cell phones, are telephones that have shortwave analogy or have digital transmission capabilities that allow users to establish wireless connections to nearby transmitters available. As in case of WLANs, the transmitter's span of coverage is called a “cell.” As the cell phone user moves from one cell to the next, the telephone connection is effectively passed from one local cell transmitter to the next transmitter available.
Now a day’s cell phone is rapidly evolving to integration with PDAs, thus providing users with increased wireless e-mail and Internet access.

1.5 Wireless LAN Overview

WLAN industry and the WLAN technology date back to the mid-1980s when the Federal Communications Commission (FCC) first made the RF spectrum available to industry.. Today, WLAN technology is experiencing very rapid growth. The main reason for this growth is the increased bandwidth made possible by the IEEE 802.11 standard.



Characteristics	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11 Mbps (11b), 54 Mbps (11a)
Data and Network Security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for 802.11i.)
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.[9]
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

Table 1.2 Key characteristics of WLAN [3]

Frequency and Data Rates

In order to provide wireless networking technology like the wired Ethernet that has been available for many years, IEEE developed the 802.11 standards. Basically the most widely adopted member of the 802.11 is IEEE 802.11a.
It operates in the range of 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM) technology. The most 802.11b standard operates in the unlicensed 2.4 GHz–2.5 GHz Industrial, Scientific, and Medical (ISM) frequency band using a direct sequence spread-spectrum technology.
The transmission speeds which 802.11b WLAN technology permits is up to 11 Mbits per second. Original IEEE 802.11 sends data at the rate of only 2 Mbps,obviously very low as compared to it .

1.6 BENEFITS

WLANs have many benefits in which four are primary which are:

1.6.1 Flexibility

Its users can enjoy the flexibility of installing and taking down WLANs in locations where necessary. Users can quickly install a small WLAN for temporary needs such as a conference, trade show, or standards meeting.

1.6.2 User Mobility

With the help of wireless networks, without physical connection with wires, its users can access internet, files and network resources. Users can be mobile along with retain high-speed, real-time access to the enterprise LAN.

1.6.3 Rapid Installation

On wireless networks we don’t need wires or cables for making new connections by drilling or pulling wires through roves walls or through ground which even requires modifications in the infrastructure cable plant .So time required for installation is reduced.

WLANs are often cited as making LAN installations possible in buildings that are subject to historic preservation rules, there are also many other examples.

1.6.4 Scalability

In order to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area, WLAN network topologies can easily be configured.

1.7 WIRELESS PERSONAL AREA NETWORKS (WPAN)

Basically wireless personal area networks are used to convey information over short distances among a private, group of participant devices. A connection made through a WPAN involves little or no infrastructure or direct connectivity to the world outside the link, unlike a wireless local area network (WLAN).

1.7.1 BLUETOOTH

Basically the IEEE 802.15.1 standard specifies the architecture and operation of Bluetooth devices, but only as far as physical layer and medium access control (MAC) layer operation is concerned. Piconet which is A Bluetooth network can allow the interconnection of eight devices in a radius of 10 meters. This network may be fixed or conditional. In a Pico net, the Master seeks the devices in its associates by emitting requests around. Then the slave answers with its own identification number. Up to 10 Pico nets can overlap to form a Scatter net, linking up to 80 Bluetooth appliances. And beyond this, the network saturates .By default; Piconets transmit only up to 10 meters. However one can increase its range up to 100 meters by increasing the power output of 100 mw (mill watts), as opposed to the 1mw of default Bluetooth.

1.7.2 Issues with PANS

The one of the biggest initial issue will simply be to equip devices with software to enable the PAN connection. But this will occur once only because technology such as Bluetooth is cost effective and available in large quantities for operation.

One biggest issue with PANs is the ability for devices to inter-operate with one another. However for pre-established networks it is not so big issue it big issue only for inter-vender equipment connections.

1.8 WIRELESS WIDE AREA NETWORKS (WWANs)

As compared to wireless LANs, Wireless WANs cover a very much more extensive area. In shortly WWANs allow users to maintain access to work-related applications and information while away from their office. As in wireless WANs, communication occurs through the use of radio signals over analog, digital cellular, or PCS networks, although signal transmission through microwaves and other electromagnetic waves is also possible.

1.9 CELLULAR GENERATIONS

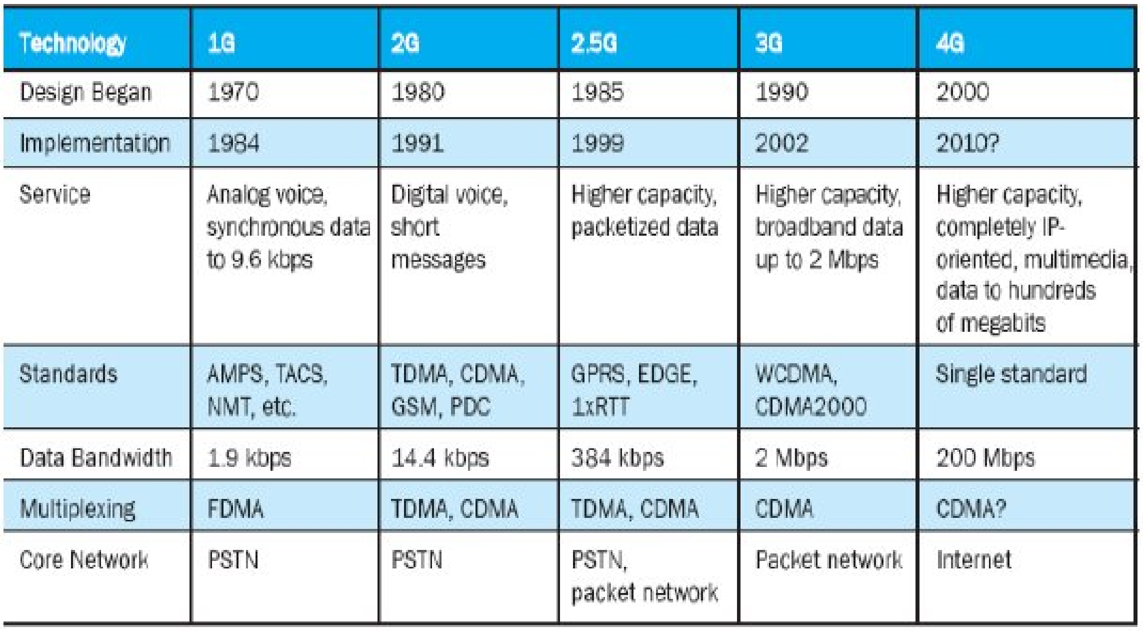
Cellular systems were based on typical or conventional cellular architecture and used direct analogue modulation for the transmission. Its different systems were working in different countries with a transmission rate of around 2.4 kbps. They had some drawbacks which were sorted out or tried to be solved in their future generations. Their voice quality was very poor and also they used unsecured unencrypted communication, which resulted in the spoofing of identities. At the same time they also had a low traffic density of a cell per radio channel and their communication mode was based on circuit switching standards.

Second generation cellular systems were developed late eighties. These designed systems were mainly used to transport voice data or traffic on the digital link, at this time. They were the first digitized systems including digital signal processing and they provided circuit, which switched data communications at a low speed. The initial success in these systems led to a competitive rush to design digital systems, but this resulted in the implementation of a variety of incompatible standards all over the world such as GSM (Global System for Mobile) mainly in Europe. TDMA (Time Division Multiple Access, IS-54 / IS-136) in the US and Personal Digital Cellular (PDC) in Japan and another system in the US named CDMA (Code Division Multiple Access, IS-195).

All these systems are operational in different parts of the world but the data rate they provide to their users was limited. There were some interim steps, before directly jumping to third generation systems that were taken between 2G and 3G, the 2.5G systems. Actually this enhancement is done to provide increased capacity and higher throughput for data service up to 384kbps. The most the importance of this generation is the optimization of channels for packet switched data to provide access to internet, whether its through mobile phone, PDA or laptop.

But still the data rates of 2.5G are not enough. So in the 1990's organizations have started working towards the launch of 3G systems, which could eliminate the drawbacks associated with previous generations and will emerge as a truly global system. These systems provide high voice quality and broadband qualities up to 2Mbps.

Although, the 3G provides high data rates but at the same time the user's needs are arising for higher access speed multimedia communication in today's environment. And another feature of seamless integration of different standards all over the world and mobility support reinforces the fact that this is the right time to start work towards implementing beyond 3G systems. Because according to historical indication, generation revolution occurs once in a decade.



Technology	1G	2G	2.5G	3G	4G
Design Began	1970	1980	1985	1990	2000
Implementation	1984	1991	1999	2002	2010?
Service	Analog voice, synchronous data to 9.6 kbps	Digital voice, short messages	Higher capacity, packetized data	Higher capacity, broadband data up to 2 Mbps	Higher capacity, completely IP-oriented, multimedia, data to hundreds of megabits
Standards	AMPS, TACS, NMT, etc.	TDMA, CDMA, GSM, PDC	GPRS, EDGE, 1xRTT	WCDMA, CDMA2000	Single standard
Data Bandwidth	1.9 kbps	14.4 kbps	384 kbps	2 Mbps	200 Mbps
Multiplexing	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	CDMA?
Core Network	PSTN	PSTN	PSTN, packet network	Packet network	Internet

Table 1.3

1.9.1 FIRST GENERATION

NMT LAUNCH

NMT is known as Nordic mobile telephone and it is the basic building step for cellular evolution. These were analogue systems basically with only limited coverage per cell and much budgeted data rate. They also can be characterized as low density systems.

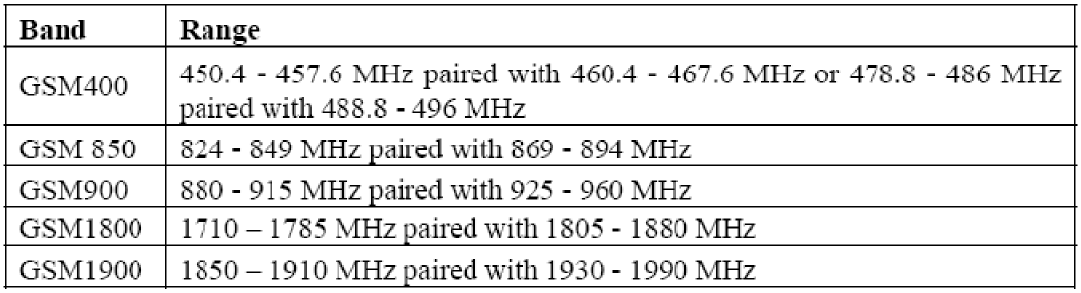
1.9.2 SECOND GENERATION

GSM LAUNCH

The basic idea which is behind the GSM is to develop a uniform standard worldwide so as to provide roaming facilities between different countries. And this technology now caters around 70% or more of all digital mobile telephony subscribers worldwide.

The data (voice) transmission rates provided by GSM initially ,is 9.6 kbps but they can be increased up to 14.3 kbps by some error correction techniques. GSM use time and frequency division multiplexing techniques, we rather call them access techniques. Both of these standards ensure the splitting of frequency band both in time slots as well as frequency channels, so as to increase the efficient use of available frequency range.

The following table shows the different operating frequency ranges for GSM.



Band	Range
GSM400	450.4 - 457.6 MHz paired with 460.4 - 467.6 MHz or 478.8 - 486 MHz paired with 488.8 - 496 MHz
GSM 850	824 - 849 MHz paired with 869 - 894 MHz
GSM900	880 - 915 MHz paired with 925 - 960 MHz
GSM1800	1710 – 1785 MHz paired with 1805 - 1880 MHz
GSM1900	1850 – 1910 MHz paired with 1930 - 1990 MHz

Table 1.4: GSM Frequency Ranges [5]

1.10 SECOND TO THIRD GENERATION BRIDGE

1.10.1 GPRS

We can be defined as the building block from 2G to 3G and due to this, this technology has been also termed as 2.5G.Therefore it seems as an enhancement of GSM systems with an increasing data rate by overlaying a packet based interface on the existing circuit switched GSM networks, giving its subscribers a choice between circuit and packet switched applications. Data rates have taken a step further to 164 kbps by the packet switched resource allocation and this technique is known as General Packet Radio Service(GPRS) also known as GSM2+.

This was thought to be a perfect evolution of GSM but rather not because it was very difficult to provide the inter linkage between the high speed circuit switched data and packet switched data .The notion of packet switching in cellular networks have become visible with the launch of this technology at the same time. It has also improved the roaming functions, now the subscribers can use the services of other service providers, even abroad. GPRS is very important in terms of channel allocation because when its user wants to use the service a time slot is reserved for the communication and when the transmission is over this slot can be used by the other user. The maximum transmission data rate available when all the eight slots are occupied is 174 kbps.

1.10.2 EDGE

The improvement in the above mentioned system is known as Evolved GSM or Enhanced Data Rates for GSM Evolution (EDGE). So this improvement has been embedded in the current setup of GSM network with higher level modulation and allows much faster data rates with transmission speed reachable to 384 kbps. EDGE has more advantage over GSM because of its modulation technique, GSM uses GMSK (Gaussian Minimum Shift key) which sends only 1 bit per symbol and it is the most efficient mode of frequency shift key. But EDGE uses 8-PSK (Phase Shift Keying) which sends 3 bits per symbol resulting in a three fold increase in the data rate but the disadvantage is that, at the expense of interference and noise.

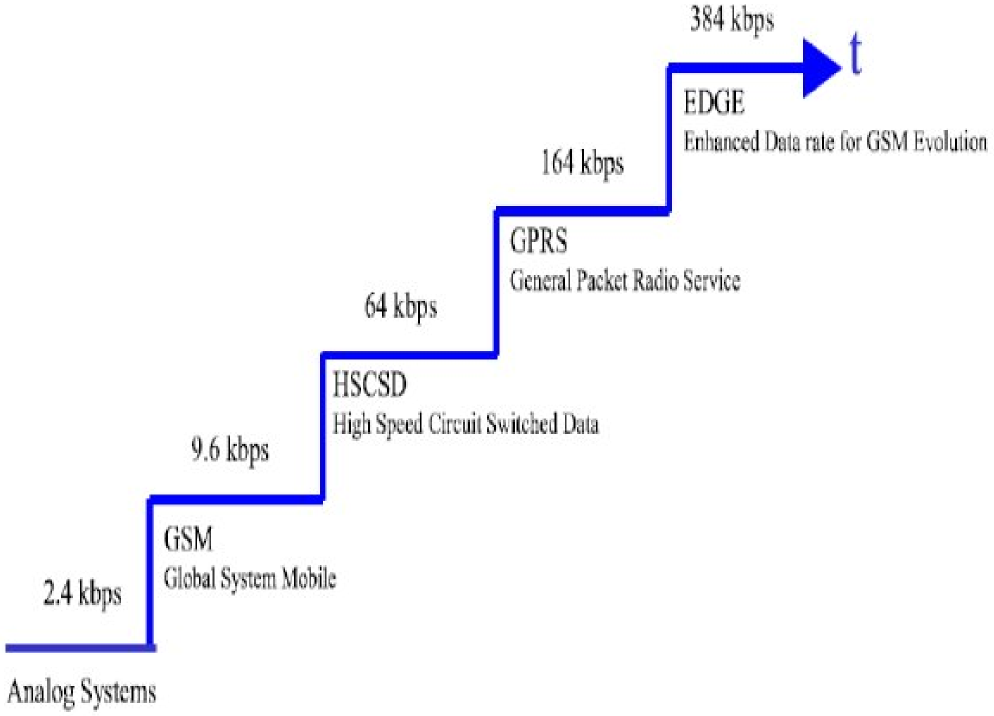

384 kbps
t
EDGE
Enhanced Data rate for GSM Evolution
164 kbps
GPRS
General Packet Radio Service
64 kbps
HSCSD
High Speed Circuit Switched Data
9.6 kbps
GSM
Global System Mobile
2.4 kbps
Analog Systems

Figure 1.3 [6]

1.11 THIRD GENERATION

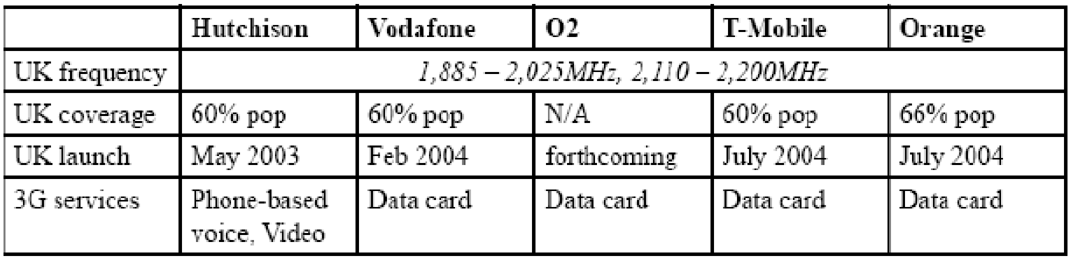
1.11.1 UMTS

The communication systems which are mostly included in third generation Universal Mobile Telecommunication system are:

- Satellite radio systems
- Paging
- Cordless radio systems
- Cellular radio systems
- Private mobile radio systems

Basically these systems were designed to fulfil the requirements which were not achieved in the previous generations and the terminal speed that can be reachable in this system is 500 km/hr. Initial transmissions for UMTS will take place in 1GHs band spectrum at a rate of 2 Mbps in low mobility conditions where as for higher coverage or wide area coverage it will be between 144 and 384 kbps. Actually these higher data rates also have opened new horizons for the mobile telecommunication. This 3G network makes use of WCDMA) multiple access technique to provide multimedia services to its customers. At the same time some 3G operators make use of ATM (Asynchronous Transfer Mode) for their over the air network with IP as their backbone network.

The following table shows the list of licensed 3G operators in the UK up to 2005.



	Hutchison	Vodafone	O2	T-Mobile	Orange
UK frequency	*1,885 – 2,025MHz, 2,110 – 2,200MHz*				
UK coverage	60% pop	60% pop	N/A	60% pop	66% pop
UK launch	May 2003	Feb 2004	forthcoming	July 2004	July 2004
3G services	Phone-based voice, Video	Data card	Data card	Data card	Data card

Table 1.4 [6]

1.12 FOURTH GENERATION

Next level of evolution in the field of wireless communications is 4G or beyond 3G.4G system will provide a complete replacement for existing communication networks. It is expected that it will provide full and secure solution, where facilities as voice, data and streamed multimedia will be provided to its users everywhere and at every time. All around the world 3G is used by mobile broadband providers, but its 4G but its 4G which will provide faster access to the internet.

Actually 4G is being developed to provide the quality of service, multimedia messaging service, video chat, mobile TV etc.

Infrastructure and the terminals of 4G will have all the standards from 2G to 4G, its infrastructure will only be packet bas

CH NO: 2

2. Security Aspects of the Wireless Systems:-

In the wireless systems the security issue has become quite essential due to the large number of people dependant on these systems in their daily life.

2.1 NEED FOR SECURITY

A wireless local area network is implemented as a substitute to the wired local area network. As the general purpose connectivity purposes Wireless LANS are becoming more widely recognised alternative for a broad range of business customers. But one of the most drawbacks is that the wireless LANS are insecure and the data sent through them can easily be broken and modified. In wireless networks the security is much more critical and compulsory than the wired networks simply because when the data is sent over the wireless network, is actually broadcast for the neighbourhood to hear. The wireless systems should not be used where critical data is sent over the airwaves, unless some countermeasures taken.
A definite and specific level of security is compulsory in all the wireless systems. If the sensitive data like those on the networks of financial institutions, banks, military networks or data concerning to terrorists etc. is sent over the wireless system then extra measures should be taken for the privacy and confidentiality otherwise one can imagine how things useful became dangerous.

2.2 Attacks on Wireless Networks

The attacks on the wireless systems and networks can be classified and divided into two categories active attacks and passive attacks.

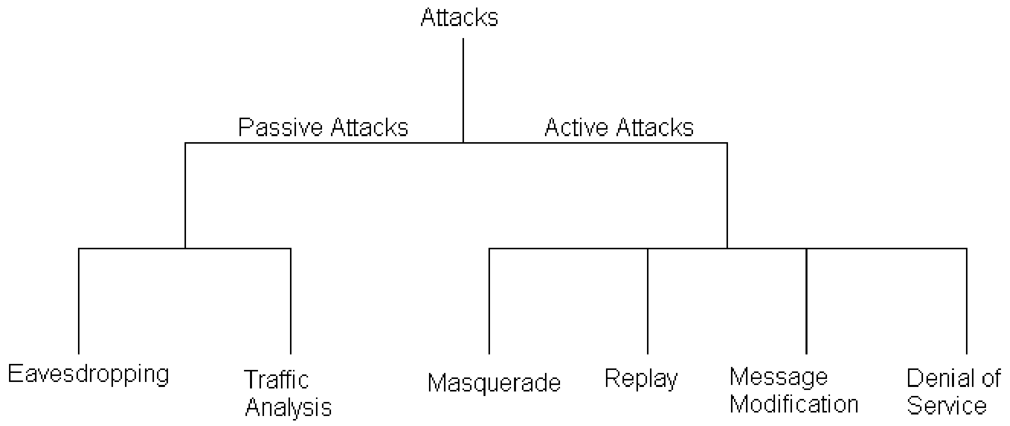


Figure 2.1

2.3 Classification of security attacks

2.3.1 Masquerade

A masquerade attacks occurs when an entity pretends to be another entity.

2.3.2 Reply

Reply is the passive capture of a data unit and its retransmission to construct the unwanted access.

2.3.3 Modification

Modification of messages means that a certain portion of message has been changed or that the messages are delayed to produce an unauthorised access.

2.3.4 Passive attacks

Passive attacks are basically eavesdropping or spoofing on information in which the attacker tries to access the transmission illegally that is being transmitted. There are two subclasses as well that are,

2.3.5 Release of message contents

In these attacks, the attacker reaches the email messages or the file that is being transferred.

2.3.6 Traffic analysis

In this attack, the attacker can discover the location and identity of communication hosts and also can observe the frequency messages and length of the messages being exchanged which could be useful if it show the useful information in guessing the nature of the information being exchanged.

2.4 AN IDEAL SECURITY SYSTEM

An ideal security system should possess the following characteristics for present but may be different for future.

2.4.1 Integrity

This means that the different operations such as substitution, insertion or deletion of data can only be performed by authorised users only.

2.4.2 Confidentiality

This means that the network system can only be accessed by authorised users. This access can be read only access. The other sort of access is the privileged access where viewing, printing, or knowing the object is permitted.

2.4.3 Denial of Service

This means that the authorised user is not prevented or denied access to objects to which it has legal access to and it applies to both service and data. The effectiveness of access control is based on two ideas, user identification and protecting the access right of the users.

2.5 Wired Equivalent Privacy WEP Protocol

As the name indicates that the goal of WEP is to provide the level of privacy on the wireless system that is equivalent to that of the wired LAN. It is a scheme to protect the IEEE 802.11wireless networks. Actually this protocol was designed to provide confidentiality for network traffic using wireless protocols. Basically WEP depends on a secret key which is shared between a mobile station and an access point as well.

The packets are encrypted by using the secret key before transmission, and an integrity check is used to ensure that packets are not modified on the way during transmission. However in reality most of the installations use a single key which is shared in between all mobile stations and access points

More sophisticated key management techniques can be used to help defend from the attacks. But there are several serious weaknesses which were identified by cryptanalysts, with the help of readily available software a WEP connection can be cracked within a few minutes. In 2003 WEP was superseded by WI-FI protected access.

In WEP RC4 encryption algorithm is used, which is known as a stream cipher. The sender XORs the key stream with the plaintext to produce cipher text. The receiver generates an identical key as he has copy of the same key. XORing the key stream with the cipher text extracts the original plaintext.

For the 802.11 standard, the open system authentication is the default form. This scheme authenticates every user that requests authentication. It depends on the default set of keys that are shared between the wireless access points and the wireless devices. The users without the correct key, requesting for connection, will be rejected and only the users with the correct key will be connected. Before transmitting the data is encrypted and also the integrity check is done to make sure that the packets are not tampered on the way during transmitting.

The IEEE 802.11 standard specifies two methods in order to use the WEP. The first method provides the window of four keys only. In this, a station or an access point can decrypt packets enciphered with any of the four keys. The transmission is limited to any one of the four manually entered keys known as the default key. The second method is the key mapping table where each unique MAC address can have separate keys which are useful in a way that the cryptographic attacks on other keys are eased, but the disadvantage is that all of the keys have to be configured manually on each device.

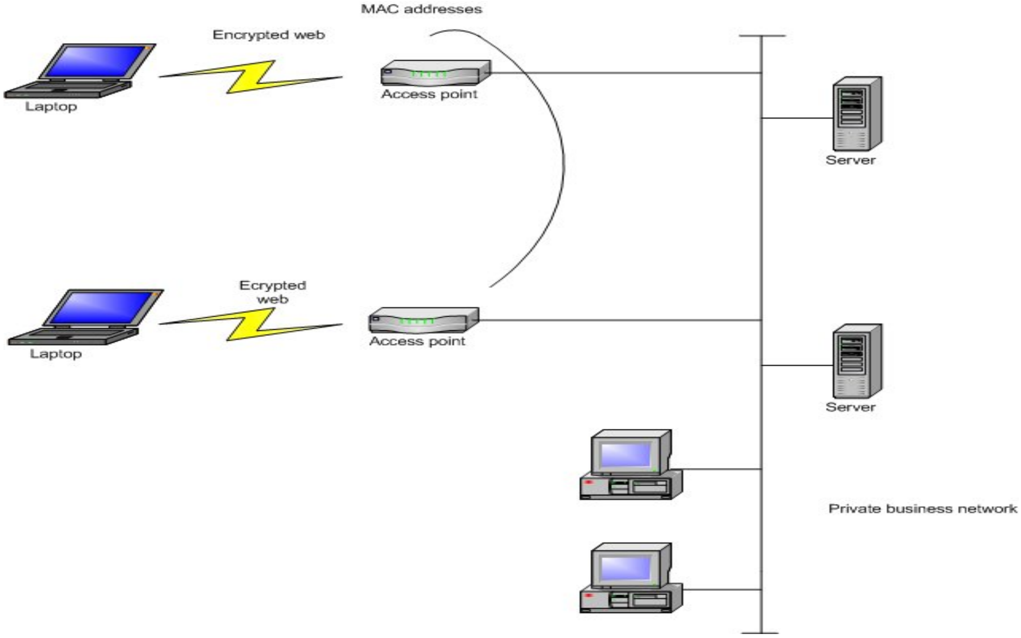


Figure 2.2 Security with access control list [8]

In the shared key authentication method the station (client) that wishing to initiate sends an authentication request management frame indicating that it desires to use the shared key authentication to the access point. The responder (access point) responds with the clear-challenge text which is the authentication management frame. Using the configuration WEP key, the client has to encrypt the challenge text and send it back in another authentication request then the access point decrypt the material and compares it with the clear text it had sent. The access point sends a positive or negative response, depending upon the comparison The WEP can be used for encrypting the data, the authentication and association. Pseudorandom Number Generator (PRNG) with the shared secret and the random initialization vector generates this challenge text. The initiator then copies the contents of the challenge text into the new management frame body. The body is then encrypted using the shared key along with the initiating vector (IV).The frame is then sent to the responder who decrypts the received frame and verifies that the Cyclic Redundancy Check (CRC) Integrity Check Value (ICV) is valid and the challenge text matches the one that is sent in the first message. If that’s ok, then the initiator and the responder switch roles and repeat the process.

2.6 Flaws in the WEP scheme

The flaws in the WEP protocol involve the initialization vector (IV) and the RC4 algorithm, a stream cipher operates in this way that it expands a short key into a infinite pseudo-random key stream. This operation makes stream ciphers vulnerable to several attacks and hackers. If an attacker flips a single bit in the cipher text, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts on two cipher texts which are encrypted with the same key stream, then it becomes possible to obtain the XOR of the two plaintexts. Plaintext can be required by statistical attacks with the help of this XOR knowledge.

In order to ensure that a packet has not been modified on the way in transit, it uses an Integrity Check (IC) field in the packet. In order to avoid encrypting two cipher texts with the same key stream, an Initialization Vector (IV) is used to augment the shared secret key and produce a different RC4 key for each packet.

2.6.1 Passive Attack for the Decryption of Traffic

A hacker can intercept whole traffic. When an IV collision occurs, by XORing two packets that use the same IV, the attacker obtains the XOR of the two plaintext messages. The resulting XOR can be used to gather data about the contents of the two messages. As IP traffic has a lot of redundancy predicable. This redundancy can be used to eliminate many possibilities for the contents of messages. If these statistical analysis are on only two messages then attacker even can look for more collisions of the same IV .Hence it becomes possible to recover a modest number of messages which are encrypted with the same key stream, so the success rate of these statistical analysis grows rapidly .If only once it becomes possible to recover entire plaintext for one of these messages, then the plaintext for all other messages follows directly.

2.6.2 Active Attack for the Injection of Traffic

We suppose that for one of the encrypted message, a attacker knows the exact plaintext. Then he will be able to construct the correct encrypted packets, and then he can generate a new message and by calculating the CRC-32 and by performing the bit flips on the genuine encrypted message in order to change the plaintext to the one message**.** This packet then can be sent to the mobile station or to the access point, and it will be accepted as a valid packet.

A slight little alteration to this attack makes it much more menacing. Even one has not the complete knowledge of the packet, it is possible to flip selected bits in a message and can then successfully adjust the encrypted CRC), to obtain a correct encrypted version of a modified packet. If an attacker has a partial knowledge about the contents of a packet, then he can intercept this packet and he can perform selective modifications on it.

2.6.3 Active Attack from the Both Ends

For the decryption of traffic signals ,the attacker makes presumption regarding the headers of a packet but not about its This information about the header is usually quite easy in particular to obtain or , all that is necessary to guess is the destination IP address .When the attacker Equipped with this knowledge ,he can flip suitable bits to transform the destination IP address and send the packet to a machine he controls, somewhere in the Internet, and transmit this using a mobile station. Now most wireless installations have Internet connectivity, the packet will be successfully decrypted by the access points and forwarded unencrypted through appropriate gateways and routers to the attacker's machine, that revealing the plaintext .An attacker if has made exact guess about the TCP headers of the packet, then it may become possible to change the destination port on the packet to be port 80 and which allow it to be forwarded through most of the firewalls

2.6.4 Attacks based on Table

Basically an attacker can build a decryption table as there is only a small gap of possible initialization vectors which allows an attacker to build it conveniently, Once when an attacker learns about the plaintext for some packets, then he can compute the RC4 key stream generated by the inilination vectors IV used. This key stream can be used to decrypt all other packets that use the same IV. Using the previous techniques, the attacker can build up a table of IVs and related key streams. Once an attacker build tables, he can decrypt each packet which is sent over the wireless links, and at the same time these tables require a very small storage almost up to 15GB only

2.7 MOBILE IP

A greater degree of connectivity is almost becoming a need for the business user on the go, as PDAs and the next generation of cellular phones become more widely deployed, Network providers and cellular service providers and wanting to position wireless LAN technologies need to have a solution which will grant this greater freedom.

Users and mobile IP provide want to maintain their home IP address while roaming beyond their home subnet. This enables transparent routing of IP datagram's to mobile users during their movement, so that data sessions can be initiated to them while they roam. This also enables sessions to be maintained in spite of physical movement between points of attachment to the Internet or other networks.

Redirection attacks are the only security problem while using this mechanism. The home agent is informed, the user has a new care of address and all IP datagram's are addressed to the actual user is redirected to the malicious user.

The Mobile IP is designed to resist two kinds of attacks:

1. A malicious user that may reply to old registration messages and cut the nodes from its network.

2. A node which may pretend to be a foreign agent and send a registration request to the home agent in order to divert traffic that is intended for the mobile node to itself. Message authentications and proper uses of the identification field of the registration request and reply messages are often used in order to protect mobile IPs from these kinds of attacks.

2.8 VIRTUAL PRIVATE NETWORKS (VPN)

Basically a virtual private network is a extension of a private network. A Virtual Private Network enables us to send data between two computers or network across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.

Concerning the users, it is point to point connection between the user's computer and corporate server. With the help of VPN connections users which are working at home or on the road can connect in a secure fashion to a remote corporate server by using the routing Infrastructure provided by a public internetwork.

2.8.1 ADVANTAGES of VPN

Main advantages of VPN are the following

Security:

As VPN is using a advance scheme for encryption and authentication, it can secure data from unauthorized persons and hackers as well.

Scalability:

The VPN enables organizations to use the Internet infrastructure within the ISPs and devices remain in the cost effective manner enabling organizations because to add large amount of capacity.

Compatibility with broadband technology:

This technology allows the telecommuters and mobile users to benefit from high speed access techniques such as cable modem and DSL to get access to their organization network and these connections are very helpful in provide a cost effective solution for connecting remote office

They have low administration requirements.

Until the VPN authentication is performed, the traffic to the internal network remains isolated.

MAC address list management and WEP key become optional due to the security measures are done by the VPN channel itself.

2.8.2 DRAWBACKS

The main drawbacks of the present VPNs are these:

Firstly it has lack of support to multicasting and roaming between the wireless networks.

And secondly, they are not completely transparent as the users receive login dialogs when roaming between VPN servers on the network and also when a user resumes from a standby mode.

2.9 Protocols associated with VPNs

In order to assure security, various tunneling protocols are used which are as under;

2.9.1 Point-to-Point Tunneling Protocol (PPTP):

It is a Layer 2 protocol which encapsulates point-to-point (PPP) frames in IP datagram's for transmission over an IP internetwork, such as the Internet. For remote access and router-to-router VPN connections, PPTP can be used .It (PPP) offers authentication as well as methods of privacy and compression of data. The Point-to-Point Tunneling Protocol (PPTP) uses a Transport control protocol (TCP) connection for tunnel maintenance and a adapted version of

Generic Routing Encapsulation to sum up PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted and/or compressed.

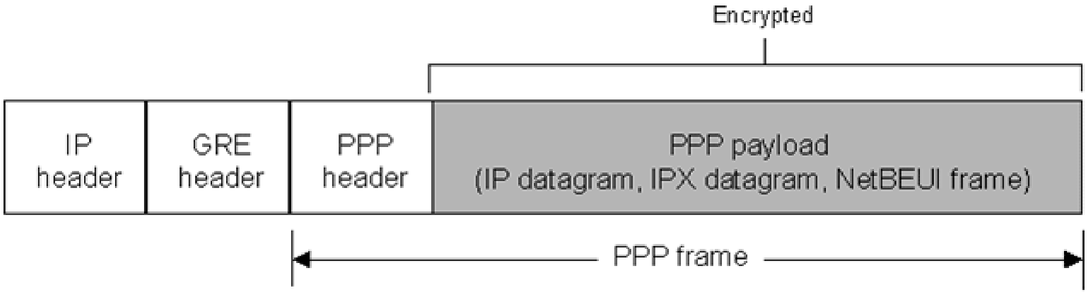


Figure 2.3 PPP Tunneling Protocol Packet [10]

2.9.2 Layer 2 Tunneling Protocols

The Layer 2 Tunneling Protocol and PPP tunneling Protocol are quite similar but there is only difference that Layer 2 Tunneling Protocol does not include any encryption or authentication mechanism. The major difference between L2TP and PPP is that L2TP combines the data and controls all channels and runs over the User Datagram Protocol (UDP). L2TP sums up PPP frames which are sent over IP, X.25, Frame Relay, or networks of Asynchronous Transfer Mode (ATM). L2TP can be used as a tunneling protocol over the Internet, when configured to use IP as its transport layer. L2TP over IP internetworks uses UDP and a series of L2TP messages for tunnel maintenance. L2TP also uses to send L2TP-encapsulated PPP frames as the tunneled data. The payloads of encapsulated PPP frames can be encrypted and/or compressed.

By combining these two channels and using high performance User Datagram Protocol (UDP), L2TP becomes more powerful which makes L2TP more firewall friendly than PPTP. This is the main advantage because most firewalls do no support GRE.

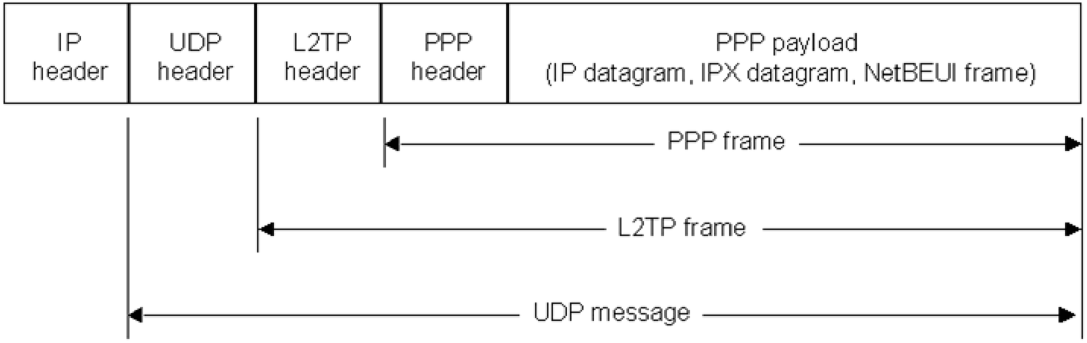


Figure 2.4   L2TP frame

2.9.3 Internet Protocol Security (IPSec)

It is basically an open standard it is based on network layer 3 security protocols. Across an IP internetwork IPSec supports the secure transfer of information and protects the IP data grams by defining the methods of specifying as how the traffic is protected and to whom it is sent. IPSec protocol either uses Encapsulation Security Payload (ESP) or Authentication Header (AH) protocols in order to protect datagram’s.

CH. NO: 3

3. What is a Malware?

Malware is software which is designed to damage a computer system without any information. Many normal computer users are however still unfamiliar with the term, and most never use it. In this chapter, we look at the various viruses that are affecting wireless communication especially mobile phone viruses. Today’s possible targets for malicious programs are: wireless networks; Mobile phones; PDAs; and vehicle-based computers, including all satellite communications. VoIP is also considered to be a prime target. Text information can be embedded into jpegs and other formats, digital photographs are ideal tools for virus writers.

Basically “Malware” stands for malicious software and typically its used as a single term to refer to any software which is designed to create damage to a single computer, server, or computer network, whether it's a virus, spyware etc. Basically it so designed so that it produces damage or disturbs computers and other devices. If malware is allowed to enter in a computer, it can cause serious damage to a computer or network and place sensitive information at risk without the owner's consent.

Malware is divided up into five **main** categories;

- Worm
- Virus Hoaxes
- Hoaxes
- Trojan
- Potentially Unwanted Programs (PUPs)

3.1 Virus

Malware has several types and Viruses are one of them. A virus is basically a “program that copies itself without a user’s consent”. It is a self-reproducing automation program and it spreads rapidly with the passage of time by inserting copies of itself into other executable code or documents.

One kind of virus which is called mobile phone viruses actually a computer virus specifically adapted for the cellular environment and it’s designed to spread from one vulnerable phone to another. It is a piece of code or program that is loaded onto a mobile device without the user’s knowledge and wish, and it runs against its will. Most of the viruses can also replicate themselves. A simple virus that can produce copies of it is relatively easy to produce. Such a simple virus is very dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one which is capable of transmitting itself across the networks and bypassing security systems.

3.1.1 File viruses

A virus that replaces a key system file on your computer is called a file virus. These viruses reload themselves, when we start our computer every time. If once it enters in our computer or in any other programs, they may spread themselves by producing it new files

3.1.2 Boot sector viruses

This is an early type of computer virus. This type virus spreads by hiding themselves in an invisible location on hard drive or floppy disk. When a computer reads an infected floppy disk, the virus is copied from the disk to your computer's memory and from there, it writes itself to the 'boot sector' on your hard drive. Each time you turn your computer on, the boot sector is read. So the virus is constantly reloaded and can copy itself on to other floppy disks. As they are easy to catch, these viruses are fairly rare nowadays.

3.1.3 Macro viruses

Macro viruses are that which infects word processor files, such as Microsoft Word documents etc. As compared to other malicious programs it is not so much dangerous but it has ability to spread rapidly by those files which are sent by emails. After an initial scare, Microsoft added protection into later versions of Word, so a user receives a warning about infected documents.

3.2 Worms programs

A worm is basically a self-contained program or combinations of programs which has ability to spread its copies functioning or segments of it into other computer systems. This propagation mostly takes place via network connections or email attachments. Worms which spread by mobile devices to other devices by memory card or Bluetooth USB are called Mobile worms. Actually it is a self standing program with no need for a host. Its characteristics include self replication and propagation. They are often designed to exploit the file transmission capabilities. Virus cannot propagate by itself whereas worms can, is the main difference between a computer virus and a worm. A worm uses a network to send copies of it to other systems and it does so without any intervention. In general, worms consume bandwidth and harm the network, whereas viruses infect or corrupt files on a targeted computer. Worms can spread via emails sent over the Internet or via corporate networks. Worms are becoming an increasing threat because as a growing number of computers are permanently connected to networks.

3.3 Hoaxes

Actually Hoaxes are false reports, which mostly claiming to do impossible damage about non-existent viruses. Unfortunately some peoples urgently believe a hoax to be a true virus warning and may take different actions such as shutting down their network. The virus hoax came about after friends they sent each other emails about a new virus threat. Someone decided that they could cause just as much trouble by sending out file warnings which real viruses can do. Hoaxes may be harmless, but they do a great deal damage to the Internet as a whole. Companies may spend a lot of money and waste their costly time what is just someone's idea of a joke or real.

3.4 Trojans

A virus which can opens your computer up to malicious intruders and then allowing them to read your files is called Trojan Virus. It does not replicate or propagate. As a Trojan contains malicious software, it can crash cell phone system components. The Trojan horses target only those cell phones which use Symbian system, which is an advanced operating system that competes with similar software from Microsoft to bring PC-like capabilities to phones. Trojan horses do not replicate themselves, like viruses but they can be just as destructive. However, they may contain a package which is armed with several malicious applications, like viruses or worms that can spread by themselves and affect other mobile devices or even computers.

3.5 Potentially unwanted programs

These can be an adware/spyware, key loggers, password crackers, etc.

3.5.1 Spyware

Spyware is basically a technology that helps in gathering information about any person or organization without their knowledge and awareness. On the Internet, spyware is programming that is put in someone's computer which secretly gather information and other data about the user and relay it to advertisers or other interested parties. Spyware is typically used by advertisers for marketing purposes but it can also be used by others for fraudulent activity. Spyware is often installed on a user’s computer in combination with a selected free-download, but it may also be installed just by visiting a website.

3.5.2 Key loggers/ Password crackers

Basically these are programs that extracts (obtains or gets) the keys and passwords with the help of which one can enter a restricted area that is only authenticated for the designated user.

3.6 A Look at Mobile Viruses

Basically a mobile virus is an electronic virus whose targets are mobile phones or wireless enabled PDAs. According to some security experts, the focus of mobile phone vulnerability to virus infection lies in the type of phone used. The mobile phones which are using GSM technology they suffer more risk. That is way cell phones running the Symbian operating system found in popular Nokia phones.

There have been a total of more than 200 mobile virus threats that have affected the mobile phones with Palm Operating System, Symbian Operating System and Windows CE Platforms.

Most of the viruses which are targeting mobile devices to date have been proof of concept rather than fully developed attack codes. The damage done includes application disabling screen defacing and in severe cases, complete shutdown of a phone requiring a factory reset. In the next section the most common mobile phone viruses with different operating systems will be described.

Multimedia Messaging Services (MMS)

In January 2005, a new type of mobile viruses were discovered which were capable to spread itself via Bluetooth and also MMS has been causing public attention and AV firm pretend that this is the most effective way for mobile viruses to replicate themselves. It is able to generates different codes to send themselves via MMS by the scanning user phonebooks contacts that might causing other innocent users with less expose to mobile security knowledge get confused and proceed to the installation process, which is giving opportunities to cell-phone-malware to executes itself.

However, user should be aware of third party application that doesn't contain any valid certificates that might be a virus (faked games, applications and security patches at Warez /Shareware site).

3.7 PALM OS Viruses

For the Palm handheld computer, the two most prominent viruses have appeared. In these two, the first one is called Liberty which tried to delete all the applications stored on the device but could not spread from Palm to Palm at the same time. The second is called Phage which was only ever seen in the laboratory.

There are three viruses which are associated with Palm OS which have cause real trouble to the Palm OS devices.

3.7.1 Liberty

Liberty was discovered in 2000 and it deletes applications and files. One of its characteristics is that it places the virus code at the end of the file, but the virus also overwrites the first 120 bytes with code and a particular message.

3.7.2 Phage

Infect Phage is the first real virus for the Palm OS PDA operating system and it deletes applications and files. Its way of working is overwriting the beginning of Palm executables. The host files are destroyed in the process. Once one infected PRC file is transferred to Palm, and then the virus keeps spreading to other Palm programs until they are all infected and destroyed.

3.7.3 Vapor

This virus deletes applications and files but at the same time it does not itself. It is basically a Trojan written for Palm OS operating system.

This Trojan hides the all installed applications but does not destroy the applications when it is activated. As the applications are not visible but the launcher window still remains in the device which could be seen from the memory information.

3.8 Overview of Threats and Possible Damage

For less desirable applications the wireless voice and data communication presents the opportunity. Due to rapid spread of wireless communications new opportunities for hackers, dissatisfied employees, and others to prove their ability in spreading viruses and malicious code is present.

3.8.1 Damage a virus can cause to a cellular phone

The present cellular phone viruses have only a little impact to users. In order to increase threat, the malware authors works continuously on it so that users have to buy their anti-virus software.
This information can be deleted, modified or stolen. In a future scenario, therefore, it is most important not to ignore the risk of attacks designed to seize valuable information, be it personal or professional.

One of another disturbing threat is ***spamming***. In the near future it seems that cellular phones may become valid tools for the propagation of unwanted SMS and MMS messages. That is way that mobile devices could become the primary device for the spreading of viruses aimed at infecting a large number of cellular phones that, once hit, would start sending unwanted spam SMS and MMS messages to all the numbers listed in the phone by the user: all this while the unaware user is charged for the costs of this fraud.

Basically other way of propagating can be through the sending on infected messages, opening TCP/IP connections directly from the applications and offering greater opportunities for the malware to spread. The risk is limited, for traditional cellular phones that do not use an open operating system such as Symbian OS. The susceptibility of wireless devices to viruses and malicious code threats appear to follow the same patterns of vulnerabilities that the wired world has experienced.

The threats to the wireless community can be divided into three groups:

- Threats based on applications
- Threats based on contents
- Mixed threats based on applications and contents

3.8.2 Threats based on application

In the wireless communication field, application-based threats are by executable malicious code that latches on to existing, or new wireless applications .When a software is downloaded from Internet or received from a unknown source, these threats are present
As we know that the first malicious application-based program that targeted the Palm operating system (OS) used in Palm Pilot personal digital assistants (PDAs) was called Liberty Crack.
Basically, Liberty Crack is designated a Trojan horse as it masquerades with one purpose, while harboring a surprise purpose.

3.8.3 Threats based on Contents

In this type of content threats, content is the threat, or malicious use of the content is the major threat. While email has become the most important asset in the wireless world, it is also one of the most vulnerable to attack.
The most common content-based threats to the wireless infrastructure occur through infected email or by spam mail as well.

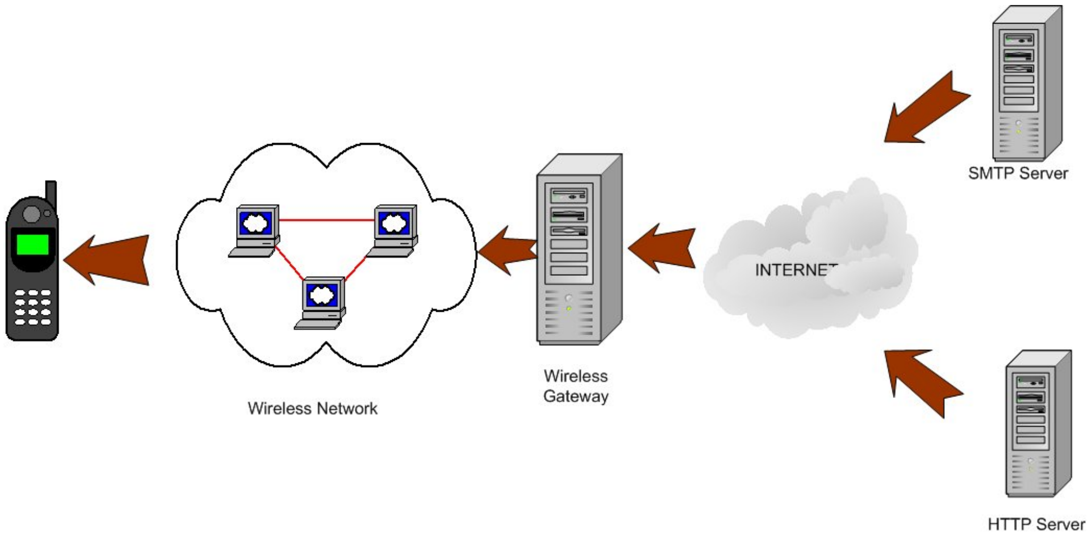


Figure 3.1 Content based threats (see [9])

The content threat to the wireless infrastructure involves email messages or spam that flow from SMTP or HTTP servers through wireless gateways to wireless devices.

3.8.4 Mixed threats based on application/content:-

In these threats, an executable program carries some malicious code, which affects the receiving device. However the spread of this malicious code is very slow as the user must download a program with malicious code and execute the program to become infected. Due to the nature of their propagation medium these threats can spread rapidly. The third type of threat is worse than the previous two types combined.

CH NO: 4

4 THREAT ASSESSMENT

In the previous chapter we discussed about the various mobile viruses, but in this, we will try to find out various solutions for the prevention of these mobile device viruses.

The risk of a mobile virus infecting thousands is increasing as handheld devices become more and more complicated. Networks of mobile phone are rapidly adopting standard net technologies that make it easier for them to offer multimedia services. But due to these changes phones become more vulnerable to some of the infection techniques used by many desktop computer viruses. Now a day's many networks are also offering *always-on* network connections to their customers that ensure they get their e-mail and text messages as fast as possible. Viruses exploit these constant connections, to spread much more quickly than they would if phones connected to data networks more occasionally.

4.1 Countermeasures

The technical countermeasures deal with the security risks identified during the threat assessment and various countermeasures are taken to protect the handheld devices from all the possible malicious attacks.

4.1.1 Authentication

The process by which you can verify that someone is who they claim they are is called authentication. Usually this involves a username and a password, as well as it can include any other method of demonstrating identity, such as a smart card, voice recognition, fingerprints or retina scan. We can explain authentication just to show visa in order to enter in other country.

So Identification and authentication (I&A) is the process of recognizing and verifying valid users, processes, or devices. Users' handheld device must be able to authenticate themselves to the handheld device by providing their password or token, or both. Security administrators should teaches or educate their users to select strong passwords. Now a day's password-cracking tools for handheld devices are available for network administrators and users for to audit their PC's synchronization application password. Today in most of the handheld devices password protection is included but it is not included in default setting. Several websites require password for downloading software's and capture it. Users should be careful about it.

Fingerprints can be attached to the handheld devices through a serial or USB port and can be set to lock the whole device, to lock an individual application, or to connect to a remote database over a network or dial-up connection. In order to authenticate the user to the device Tamper-proof smart cards are used which contain user unique identification information. Users which are using tamper-proof smart cards usually insert the smart card into a specified slot on the device and provide their password to authenticate themselves. In order to access the device the malicious users must have captured of the smart card and knowledge of the user’s password .For unique device identifiers, when available for, then they can be used as authorization mechanism in order to authenticate and to provide network access to a handheld device available. Several available methods can be used by handheld devices to identify a unique handheld device, which includes flash ID, device ID, and Electronic Serial Number as well. For two-factor authentication, Unique device identifiers can be used to authenticate the handheld device for the network access for service or all the handheld device itself to used as a physical token also.

For an unauthorized user, it will be possible to copy the shape of a signature and many handwriting judgment (identification) programs measure aspects that are more difficult to copy. However the user can also select a password for secrecy to write instead of a signature, but it is more widely available on paper documents which are distributed in the normal course of business-

4.1.2 Encryption

The process of transforming in plaintext in cryptography and to make it unreadable to anyone else except those possessing its knowledge is called usually some files on the device may require a higher level of security than password protection can offer. For example, user passwords are required to access all sorts of automated services in our everyday lives.

If we think for a while in a single day the services which we are using and think about risks we have to face and the important of encryption. In a day, a user has the need to use their passwords in order to draw money from an automatic teller machine, in order to listen to voice mail, in order to enter a building by typing an specific access code, to browse their favorite Web sites on internet, to purchase goods online, in order to access online accounts, also to make a phone call by using their calling cards, and also to access their personal and business e-mails.

The information on add-on backup storage modules should also be encrypted and the modules securely stored when not in use. An extra layer of defense is provided for further protection of sensitive information stored on handheld devices by this additional level of security. In these days a large number of free software programs are available which help their users to encrypt personal important files by enriched security.

Handheld device users may elect to encrypt files and messages before the files and messages are transferred through a wireless port.

4.1.3 Importance of Antivirus Software

It is another important security measure, for handheld devices. Regardless of their security requirements; all agencies should incorporate PDA antivirus applications to scan e-mail and data files and to remove malware from files upon transmission to the device. For better Antivirus software it is obligatory that the software must scan all entry ports for incoming traffic check their licenses and their producing agencies should regular updates its components. Generally most major PC antivirus software vendors have handheld device antivirus software that can be downloaded directly from their Web sites.

4.1.4 Public Key Infrastructure (PKI)

A public infrastructure (PKI) is an arrangement whose function is to binds public keys with their respective use identities with by means of a certificate authority. Now a day's many handheld devices are starting to offer support for PKI technologies. PKI is one of the best among all available methods for the requirement of confidentiality, integrity as well as for authentication. Asymmetric encryption method is used in Public key infrastructure it is commonly known as the public-private key method, for encryption and ensuring the integrity of documents and messages as well. A digital certificate are issued in this method by a digital assigning authority, and it can authenticate the claimed identity of people and other organizations over a public network like as in the Internet, it also establishes the level of security, the encryptions algorithms and also providing policy for its users. It contains server software and client software.

Although the use of PKI counters many threats associated with public networks but at the same time also introduces management overhead and additional hardware and software costs that should be evaluated while performing the risk assessment and selecting the appropriate countermeasures to meet the agency's security requirements.

4.1.5 VPN and Firewalls

In a wide variety of industries the organizations are mostly using handheld devices for remote access to patient records, shipping logistics and merchandise inventory .From the last a few years laptop computers and desktops secure remote access has been successfully enabled with the use of firewalls and VPN between the handheld device and the organization's network a VPN basically creates a virtual private network by sharing the public network infrastructure. The basic function of VPN technology is to offers the security of a private network through access control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks.

In order to guarantee a suitable level of security, it is compulsory to protect the mobile devices with anti-virus software complete with an automatic updating mechanism that is sent directly to the mobile device.

4.2 What is an Antivirus?

Basically an antivirus program is nothing more than a system which is used for analyzing information and then, if it finds that something is infected by viruses, it disinfects it. This information is analyzed in different ways depending on where it comes from.

Operations of antivirus are different when monitoring floppy disk operations than when monitoring e-mail traffic or movements of data over a LAN.

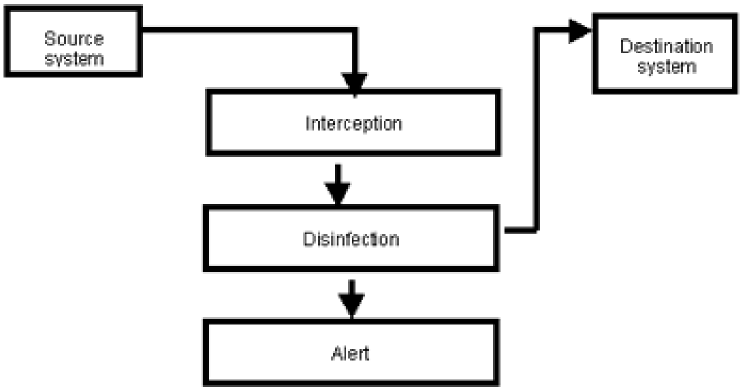


Figure 4.1

If there is no antivirus protection is available, then cellular phone users should pay particular attention before proceeding with the installation of new software or downloading new applications from the Internet, by verifying the source of the software and tracking the behavior of the phone right after the changes have been instituted.

Currently various companies are taking different measures to preventing viral infection in their handhelds. F-Secure Anti-Virus for WAP Gateways the product scans for and removes all manner of viruses from the data stream before it even reaches the handheld.

4.3 Symantec's Solution for Handhelds

Now a day for most of the handhelds devices, Symantec antivirus make secure mobile computing and it also can safeguard as well as prevents the most possible spread of viruses to the network.

Our PDA has important information which we use every day, so it protects it with virus protection developed especially for Pocket PC and Palm OS-based devices. It scans files rapidly also at the same time it uses only a little memory for it. At the same time it also protects when we download files or receive emails attachments. For handhelds Symantec Anti Virus is installed on the desktop and then synchronized to the handheld device automatically. One of its portions, On Device Alerting notifies the user when a virus is found, when virus definitions were last updated, and when additional media is detected, allowing the user to scan the contents for threats.

Basically Symantec Antivirus for Handhelds is a service which you renew annually, so you're assured of having the most up-to-date features, OS compatibility, and virus protection. Live Update technology in Symantec's exclusive downloads new virus protection updates to your PC as they become available. The next time when you synchronize our handheld with your PC, the new updates are transferred automatically. At the same time you can also get updates directly from the Internet over a wireless connection. Defend your PDA and your valuable data against viruses with Symantec Antivirus for Handhelds for handhelds Symantec Anti Virus is installed on the desktop and then synchronized to the handheld device automatically. Its users can monitor as more as one handheld device through this interface.

4.3.1 Wireless and synchronized live update support

Function of this portion is to ensure unto date virus definitions and real time security even when the user is away from the workplace. The administrators who already used internal Live Update servers for definition can configure their mobile devices to get them from the same location.

4.3.2 Threat list of known PALM OS or Pocket PC

In this the threat list of known Palm and Pocket PC viruses and virus details are stored in the virus definition file, so the users have the latest information about the known threats they suffered.

4.3.3 Activity Log

Function of the activity log is to show all the recently logged events so that to ensure that users will be aware of likely risks. This event reporting on virus activity, scan and other event history is collected, transferred during synchronization and reported through the events panel on the desktop.

4.3.4 Virus repair and file deleting option

This option enables users to remove a virus that is detected.

4.4 F-Secure Solution

Now a days "F-secure mobile antivirus" is also the most wide-ranging solution for protecting mobile devices against harmful contents. F-Secure basically provide real time device protection with the help of automatic antivirus updates by an SMS update mechanism or with the HTTPS connectivity's-secure mobile antivirus is designed in a manner as easy to use as possible.

Actually all the files are automatically scanned for viruses when they are saved, downloaded, copied, synchronized or modified in order to prevent from infection for safety. For mobile devices which have WLAN connectivity, an integrated firewall safeguards the mobile device from any type of attack whether it is intrusion or malware.

4.4.1 Automatic Real Time Antivirus Protections

When file exchange is taken place with another device, or when direct internet downloading Occur, Automatic Real Time Antivirus automatically stops viruses and malicious codes by attacking via PC synchronization, when it detects an infected file it is immediately quarantined to protect all other data in the system.

4.4.2 Integrated Firewall Protection

In the case of smart phones pure antivirus solutions are not enough that access open public networks such as WLAN .Now a day the new generations of mobile devices are in many ways like portable PCs and should be protected with a firewall. Thus the firewall scans both incoming and outgoing data packets and stops malicious, unwanted, harmful or possibly dangerous packets.

4.4.3 Centralized Management for Protection Level Monitoring

By using F-secure mobile services as gateway, then the IT administrator can centrally monitor the protection status of the company smart phones. As F secure has flexibility in use so its administrator can conveniently add more smart phones into the wireless antivirus service. Administer send the service activation code as an SMS message directly to the phones, can monitor the service subscription status with the help of standard web browser.

4.5 McAFee Solution

Almost all the mobile devices that access the internet and receive or send text messages are vulnerable to malware. Therefore these devices can receive viruses during the downloading and during installing an application containing viruses. McAfee automatically secures the device with scanning and cleaning files, emails, internet downloaded text messages and other attachments of files or video clips or movies.

Without interrupting their connections applications it always remove worms, Trojans and other malicious and at the same time it also detects multiple entry points and exit points, for emails, attachments and Bluetooth.

Its Inline cleaning automatically cleans infections when viruses, worms, Trojans or other threats are found.

Moreover it also prevents the spread of virus to contacts already stored on the phone. The McAfee virus scan helps prevent the unintentional sending of infected messages and attachments to the contacts. At the same time its feature also includes automatic hassle-free updates as they run silently in the background and the expertise ensures that there is always the latest protection.

4.6 Trend Micro's Virus/Malicious Code Protection Solution

According to this, the protection solution for the wireless infrastructure must have the following attributes:
Multiple layers of protection in order to address the various entry points and transmission paths of viruses and malicious code. Centralized management integration of all antivirus solutions including maintenance of their gateway, desktop server, and device-level protection.
Within the wireless infrastructure, Implementation for early detection to minimize damage and costs.

Tools to counter the wireless threat, rather than just applying wired world tools Mechanisms for automatic maintenance, updating, and upgrading of virus protection since such protection is only as good as the last update Involve all parties via increased awareness of the possible threat including corporate IT managers, service providers, operating system and application developers, and end users. Also involve all parties via increased awareness of the potential threat including corporate, IT managers, service providers, operating system and application developers, and end users. Real mechanisms for their automatic maintenance, updating, and upgrading of virus protection, since such protection is only as good as the last update.

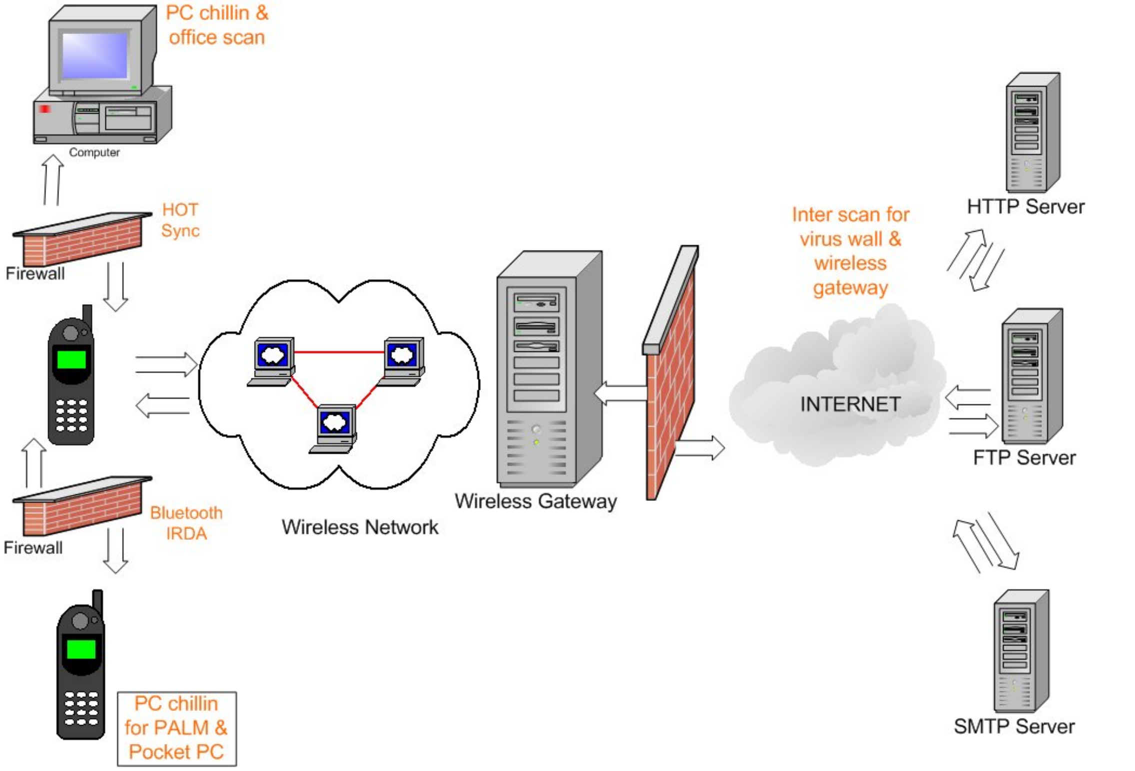


Figure 4.2 Multiple layers of protection are placed at key entry points and transmission paths in the wireless infrastructure [10]

Driven by this overall strategy, Trend Micro has released a sequence of products that address the virus and malicious code protection needs of the wireless community.

- Solutions for wireless devices
- Solutions for wireless gateways

4.6.1 Wireless Device Solutions for Device-to-Device Threats

Three vendors Symbians, EPOC and Palm developed own operating systems. Microsoft ’Pocket PC’ system represents the largest segment of present PDA market. Now a separate product is needed for each of them, in order to prevent these from mobile virus code.

Following features contains the initial release of virus software’s

1. Familiar User Interface
Basically familiar user interface contain a device-specific design that provides the look and feel of applications which are already in use offering complete control with a minimal learning curve.

2. On-Demand Scanning
Almost every wireless supported device contain its own antivirus scanner for security which can be called upon at any time to check for likely threats when they are first received in device.

3. Easy Maintenance
By using device standard process, the Product and Virus Pattern file updates are easily completed, hence making it easier for the users to keep current protection.

4. Minimal Footprint
For wireless, PC-cillin provides easy in use portable antivirus security in order to protect against threats.

4.6.2 Wireless Gateway Solutions

Basically as all emails by which we communicate, which are sent by wireless devices, all files video clips, pictures, sceneries, screen savers which we downloaded from Internet and these services are provided by some type of servers, so the protection for malicious programs and viruses must be started from these servers virus and malicious code protection for the wireless infrastructure must begin at these servers. To fulfill this need, Trend Micro has introduced InterScan VirusWall for all Wireless Gateways.In order to protect, a range of these wireless gateways from their servers software from specific threats in the wireless field. Therefore corporate administrators will install this product on their wireless gateways to protect corporate users, while service providers can install it to protect their subscribers. For Wireless Gateways Inters can Virus Wall is server-based software that builds up information flow management with virus protection at the wireless gateway, which are applicable to WAP gateways, email servers, and others. It is composed of two parts:

Virus Wall, which is to secure SMTP and HTTP traffic from viruses and malicious code.

In order to block wireless threats E Manager filters content based on keywords and phrases. For Wireless Gateways, Inters can Virus Wall incorporates intelligence for Compact HTML (CHTML) and the Wireless Markup Language (WML), which enabling detection of viruses and malicious code in these wireless Internet protocols.

At least once each week more often when really require, Trend Micro updates its virus pattern files. Its updates can be retrieved automatically or by manually.
In reality it is not enough to simply scan for known viruses and for malicious code. As both in the case of wired world and wireless word viruses and malicious codes are likely to appear for short time period .This threat can be addressed by inter Scan Virus Wall for wireless Gateways ,which is basically rule based technology and by behavioral monitoring, analysis of viruses or malicious can be done.
For explanation, for example, if the malicious code intends to dial 11911 without keys on the keypad being depressed, then this code is blocked, regardless of its exact form, as the user has decided that this is never a desirable action.

In order to include new rule sets the Manager has been redesigned, which specifically address wireless content threats such as spamming which are used by the recent Timofonica Trojan and the exploitation of security holes such as buffer overflow type vulnerabilities.

By using an updateable list of known wireless content threats, it allows new threats to be stopped proactively before pattern-based solutions can be deployed throughout the wireless network.

4.7 Security measures for WLANs

We will also look at a few security techniques that are adopted to avoid any kind of attacks to our WLANs. These measures need to be taken in order to prevent the system from intruders who can risk our system.

4.7.1 By controlling the broadcast area

As many of the wireless access points let adjust the signal strength, in which some are those which even let us to adjust signal direction as well. So we need to begin by placing the Access Points as far away from exterior walls and windows as possible, then also play around with signal strength so we can just hardly get connections near exterior walls. Even this isn't enough because the sensitive snooping equipment are available has ability to pick up wireless signals from an AP even at distances of several hundred feet or even more. So even with most favorable AP placement, there are chances that signal can leak.

4.7.2 Locking of APs

There are a lot of people who are not aware to change the defaults on their APs, and maintaining the default administrator password like admin for Linksys products which makes the system a good target a strong password to protect each AP should be used.

4.7.3 Banning of Rogue Access Points

If an AP is connected to your home or office network, then make sure you or the network administrator put it there.

4.7.4 By Use of 128-bit WEP

By cracking the WEP security protocol by passive attacks is just an irritation for a skilled hacker by using Linux freeware. Still, the protocol does at least add a layer of difficulty.

4.7.5 Use SSIDS wisely

For your APs, change yours default Service Set Identifiers (SSIDs), and also at the same time don't use anything obvious like your address or company name date of birth family name. Buy APs for corporate setups, that let you disable broadcast SSID. Intruders can use programs such as Kismet to get the SSIDs anyway.

4.7.6 Limit access rights

If there are working numerous persons of different departments in a very large building then there may be many chances not every person in the building needs wireless. Once when you know who should take to the airwaves, then set your APs to allow access by wireless cards with authorized MAC addresses only.

4.7.7 Limit the number of user addresses

If you don't have a large numbers users then, consider limiting the maximum number of DHCP addresses the network can assign, allowing just enough to cover the users you have. At a time if everyone in the group adjusted tries to connect but some can't, then you should come to know that there are unauthorized log-ons.

4.7.8 Authenticate users

A firewall should be installed that supports VPN connectivity, and require users to log on as if they were dialing in remotely. One should twist the settings to allow only the types of permissions that wireless users need. In this type of assault, the performer sets up a machine that pretends to be an authorized AP, in the hope that someone will be tricked into logging on. Then if the user connect to an AP and don't get the VPN log-on prompt that is expected, then there is something missing.

So, all these measures when put together make life very hard for the intruders.

4.8 PREVENTIVE MEASURES TO AVOID MOBILE VIRUSES

As we all know that prevention is the best method to combat viruses. The general rule for protection is that, not to accept content or install applications from sources which are not trusted, especially viruses such as Cabir requires which requires the user to accept it not just once but several times before it will install and take effect. I should recommend that users do not accept files and other unknown items from sources which are not known, especially if unsure of the content. By awareness and following this advice, users can help and prevent the propagation of such viruses.

One should advise users to turn off and remove those services that are not needed. By taking the example of Bluetooth if one is using a Bluetooth-enabled mobile phone, and if Bluetooth is not required, it should be turned off, since Bluetooth is the major transportation for viruses.

If however, anyone needs to use Bluetooth, then ensure the devices' visibility setting is set to hidden so that it cannot be scanned by other Bluetooth devices.

Also avoid the use of device pairing. If it must be used, then ensure that all paired devices are set to Unauthorized such that each connection request has to be authorized by the user. Do not accept applications which have no digital signature or from unknown sources. Also you should absolutely sure of the origin and trustworthiness of the origin of the application before accepting it. By disabling the discoverability feature, Bluetooth wireless technology applications can be enjoyed safely simply. This means by doing this then they are able to use the applications and even remain unseen by other Bluetooth users in the surrounding area keeping safe from attacks and still continuing to use their Bluetooth capabilities at the same time.

It is highly unlikely that snarfers can do much damage, especially if the Bluetooth function is turned to non-discoverable mode.

4.9 The Future of Wireless Devices and Viruses

As with the passage of time the average user for the wireless technology is increasing, the demand for wireless-enabled devices will likewise increase. It has happened in most telecommunications industries that a market leader will emerge, and their platform will become the main standard in the world just like Intel and the Palm devices.

When the hardware becomes more standardized and the user base increases, then the chances will increase significantly that someone will make a virus for them, as the impact of a well-written virus would be much greater than one targeting a few hundred devices. Whose result is, it is likely that we will see an increase in the type and number of viruses/worms/exploits for wireless devices increase dramatically as these technologies become more mainstream.

An interesting question arises from the cell phone damage issue. Therefore it is entirely imaginable that other forms of attacks which include viruses and worms could be launched against a great many wireless devices. It is the responsibility of only user in past that if some ones computer infected by virus which was expected to remove it. This method is unfortunately not sustainable for the current generation of wireless devices, as most do not contain enough memory to store an up-to-date virus database, or even to have a simple mail filter setup. As mobile technology marches forward rapidly, and the demand for ever smaller portable devices continue, it would seem that the service providers are going to have to take more responsibility for protecting their customers from the evils of the general networks.

Now a day's most of the wireless devices increase their capacity to store information, data (storage) and many things may change again soon with the passage of time, so at least for the shortly we should be asking to our telecom and wireless service providers that what steps they are taking to make it possible so that our costly precious wireless devices are sufficiently protected from the cold, hot, dark dangerous world.

CH NO:5

5. CONCLUSION & SUGGESTION

As we all know that these days, there are some additional applications in the cell phones such as Bluetooth, SMS, MMS, and Wi-Fi etc. These applications make them quite vulnerable to virus writers, which for them has become a tempting target.

This project started from the description of wireless devices and wireless technologies such as WLANs, WMANs, WWANs, WPANs and the cellular generations, and the features they possess were briefly discussed.

Also then some of the security issues of the wireless systems were discussed which includes the kinds of attacks on the systems and various security protocols including WEP, Mobile IP and VPN.

The third goal of the thesis was the investigation of the viruses and the prominent list of viruses that have so far hit the different Operating Systems such as Symbian OS, PALM OS and Windows CE for Pocket PC and the threats they posed on the device.

The fourth goal was very important one in which the existing countermeasures for the prevention of these viruses and what tools we should have to use when the system gets infected with these malwares from few of the biggest firms like F-secure, Symantec and few more were looked at. Also for the prevention of these viruses few security measures were described.

In this report, the author has tried to investigate the threats of these different viruses after searching numerous articles and news about all the viruses that have hit the wireless devices over the recent times and mentioned the most prominent of these viruses as to how they entered the wireless devices, what damage they caused to the device and how they were disinfected.

Suggestion

This thesis gives us an idea about the best way to combat viruses is by knowing their existence. We after going through all the study and research regarding this project we come to know that there is to date no virus found which can *auto install* itself into a system and they use a so called *social engineering* method to spread. It is advised therefore that, not to install any applications from non-trusted parties.

All the music and games that a user wishes to download should be done from the official websites. The Bluetooth of the device should also be kept to the non discoverable mode if not in use which really makes the difficult for the hacker to get into the system for attack. Even if the application is installed by human error, there should be well up to date antivirus software which scans the system and detects the virus even before it can spread into the system.

All these factors if applied can really lead to a secure and virus free system for the users of wireless systems.

References

[1] Wireless Networks from R.Nicopolitidis, M.S. Obaidat, G.I. Papadimitriou, A.S. Pomportsis. Wiley.

[2] Wireless communication principles and fundamentals. Wiley.

[3] National Institute for Standards & Technology (NIST) Wireless Network Security, by Tom Karygiannis, Les Owens.

[4] 4 G features by Jawwad Ibrahim, Bechtel Corporation.

[5] Evolution of mobile Technology and Business models by Su En Tan, Centre for Tele-Information.

[6] Evolution towards Fourth Generation Mobile Multimedia Communication by Carlos Rodrogoez, Frits Schoute and Ramjee Prasad, Delft University Of Technology.

[7] NIST Security for Telecommuting and Broadband Communication, National Institute for Standards & Technology.

[8] IEEE 802.11b Wired Equivalent Privacy Security at :http://www.wi-fi.com/pdf/Wi-FiWEPSecurity.pdf .

[9] Virtual Private Networking, An Overview at: http://www.microsoft.com/technet/prodtechnol/windows2000serv/plan/vpnoverview.mspx

[10] Malware Theory and Methods of Protection by Brett Neilson.

Bibliography

1. Theodore Rappaport, Wireless Communications: Principles and Practice, Second Edition, Prentice Hall, December 2001.

2. Yi-Bing Lin, Imrich Chlamtac, Wireless and Mobile Network Architectures, John Wiles & Sohns, 1st edition, 2000.

3. John Edney, William A. Arbaugh,Real 802.11 Security.

4. Chris J Mitchell, Security For Mobility, IEE Telecommunication series 51.

5. C-K Toh, Ad Hoc Mobile Wireless Networks protocols and systems,

6. Chris Benton, Cameron Hunt, Network Security, Second Edition.

7. Stallings W. Network Security Essentials: Applications and Standards, Prentice Hall.

8. Stallings W. Wireless Communications and Networks, Prentice Hall 2002.

WWW Resources

1. www.ieee.org

2. www.symantec.com

3. www.f-secure.com

4. www.mcafee.com

5. www.cnn.com

6. www.bbc.co.uk

7. www.cisco.com

8. http://searchnetworking.techtarget.com

9. http://www.proxim.com/solutions/man

10. http://www.pdamd.com/vertical/features/wireless_4.xml

12. http://www.palowireless.com

13. www.itu.int

Acronyms and Abbreviations:-

1G	First Generation
2G	Second Generation
3G	Third Generation
4G	Fourth Generation
IEEE	Institute of Electrical and Electronics engineers
AMPS	Advanced Mobile Phone Systems
GSM	Global System for Mobile Communications
UMTS	Universal Mobile Telecommunication Service
GPRS	General Packet Radio Service
EDGE	Enhanced Data GSM Environment
FCC	Federal Communications Commission
ISM	Industrial, Scientific and Medical
WEP	Wired Equivalent Privacy
WAP	Wireless Application Protocol
WI-Fi	Wireless Fidelity
WWAN	Wireless Wide Area Network
WPAN	Wireless Personal Area Network
VPN	Virtual Private Network
PKI	Public Key Infrastructure
PPTP	Point to Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
IPSec	Internet Protocol Security
SSID	Service Set Identifier
SIG	Special Interest Group
OFDM	Orthogonal Frequency Division Multiplexing
MMS	Multimedia Messaging Service
SMS	Short Message Service
AP	Access Point
PC	Personal Computer
PDA	Personal Digital Assistant
CCK	Complimentary Code-Keying Modulation
PBCC	Packet Binary Convolution Coding Modulation
CE	Consumer Electronics
OS	Operating System
ARM	Advanced Reduced instruction set computer Machine