Security & Vulnerability Analysis of Wireless Messaging Protocols & Applications

Presented at Pak Con 2004
www.pakcon.org

Atique Ahmed Khan

Table of Contents

Section 1. Introduction

Abstract

Wireless messaging is now a dynamic ingredient in the communication modes of our life. Many applications over the Internet now use wireless messages to contact with the end-user. This paper describes the messaging infrastructure and the related protocols used in this scenario. It also presents many ways you can use the wireless networks to talk with your applications. There is also a growing concern over how much these services are secure and how they can be compromised, which are described briefly in this presentation.

About the author

Atique Ahmed Khan is a web developer in the country's leading stock exchange, an organization whose online system provides stock trading over the Internet. He has also developed Wireless SCADA (Supervisory Control & Data Acquisition System) to control appliances over the web, WAP and by using SMS in his graduation project. For comments about this tutorial, please contact at nimbus81@yahoo.com

Overview of this paper

Starting with a brief introduction of telecommunication infrastructure and wireless messaging protocols, the discussion will move towards the integration of wireless networks and the Internet. Some success stories of SMS-powered applications and ways to develop them are presented. Finally security threats and their effective measures to protect them are presented.

Section 2. Cellular communication networks

Reading the air

GSM (Global System for Mobile Communication) is the most common wireless system in the world. Along with the telephony services, it also provides non-voice services called data (bearer) services. These include General Packet Radio Service (GPRS) for packet switched network connection, Short Message Service (SMS) that can contain alphanumeric characters, audio and video contents, facsimile and email facility. A core GSM network contains the following components to perform the telephony/data service:

- Mobile Station
- BTS
- BSC
- MSC
- The Registers (HLR, VLR, AUC, EIR)
- STP
- SMSC

Mobile Station

This is the equipment from where the user initiates the wireless services. It can be a mobile phone or a hardware component such as GSM modem. Nowadays, many modern types of equipment can do the task to talk with the GSM network, ranging from smart phones and paging devices to PDAs and communicators. All of them resemble in the air interface and the way they receive the data from wireless network, but their features can be a lot more different.

Base Transceiver Station (BTS)

A very common sign found in the urban area is the tower painted with white and red strips. This is the Base Transceiver Station, or BTS in short. Its main functioning is to provide the air interface to the mobile equipment, that is, a pure wireless connection with the mobile phone. All the data to and from the communication network is transferred to the mobile phone using the BTS. It has a very short coverage area (or cells); so many BTSs are installed on strategic positions over the country to provide seamless service for end-users.

Base Station Controller (BSC)

Base Station Controller (BSC) provides all the control functions and physical link between the BTS and Mobile Service Switching Center (MSC). It is actually a high capacity switch providing handover among cells, control of Radio Frequency (RF) power levels in BTSs and monitors the BTSs in its Location Area (LA).

Mobile Service Switching Center (MSC)

It is the core component and the heart of cellular network. It has multi functions and some very important data resides over here. It performs the telephony switching functions of the system and controls call to and from other telephones and data systems. MSC acts like a standard exchange and performs registration, authentication, location updating, handovers, call routing to other subscribers and roaming etc. Various databases assist MSC in executing the above-described actions, commonly called registers.

The Registers

Home Location Register (HLR)
Home Location Register (HLR) is a database used for the storage and management of subscriptions. It contains permanent data about a subscriber and its profile, pointer to current Visitor Location Register (VLR), other information and activity status like whether the mobile is switched on or not. The data needed by MSC is provided by HLR includes International Mobile Station Identification (IMSI), Mobile Station ISDN (MSISDN) and current VLR address.

Visitor Location Register (VLR)
Visitor Location Register (VLR) is a database for temporary information about subscribers needed by MSC to serve visiting subscribers and mobile roaming into new MSC. It has the current location of mobile station and administration information.

Authentication Center (AUC)
Authentication Center (AUC) stores parameters for encryption to user's identity and confidentiality. It is a protected database containing the copy of secret key stored in the Subscriber Identity Module (SIM) that is used for authentication and encryption over radio channels. It is needed normally when the mobile station is turned on and with each incoming/outgoing call. An authentication will be successful if the security code at AUC matches with that stored in the SIM.

Equipment Identity Register (EIR)
Equipment Identity Register (EIR) is a database for identity of mobile equipment, preventing calls from stolen, defective or unauthorized mobile phones. It contains a list of valid mobile phones identified by International Mobile Equipment Identity (IMEI). Other lists includes:

White List: It contains good IMEIs.
Black List: It contains bad or stolen handsets.
Gray List: It contains uncertain IMEIs, whose characteristics are doubtful.
Just like black, gray and white hats!

Signaling Transfer Point (STP)

A good analogy to understand the Signaling Transfer Point (STP) is the network router, whose task is to route traffic on the Internet. An STP performs routing, address translation and failover functionality. Just like the Internet router uses TCP/IP protocol, STP uses SS7, commonly known as C7. Multiple dedicated high capacity access paths exist among several STPs for reliable connections, since they carry a huge amount of data and they are responsible for the transportation of all the traffic. With the increase in pressure of telephony and bearer services, many carriers are in need of cost-effective, high bandwidth inter-STP connections, and they are planning to migrate over IP networks using SS7 over IP SIGTRAN standards.

Short Message Service Center (SMSC)

Short Message Service Center (SMSC) is a place where all the SMS are brought before they are sent to their destination. It uses *store-and-forward* technique for SMS transfer, as the recipient mobile station may be turned off, or it could be out of range. So the SMS is stored as long as it is not delivered to the destination. Only a successful delivery to recipient or a time out (normally three days) will delete the entry from the SMSC.

`1 message received`
Take a brief look of what we have been studying in this section. Suppose a message from mobile station is written and destined to be sent to another mobile station that is turned off at the moment. The message will be received from mobile equipment by BTS and passed to BSC, MSC and the core network, until it finally reaches to SMSC. At this moment, an acknowledgement is sent to the sender mobile equipment and 'Message Sent' will be displayed over the screen of the sender. Now the message is stored in the SMSC, it requests HLR to provide the information about the recipient status. Unfortunately HLR responds that the recipient's mobile phone is switched off and tells the SMSC to wait. When the mobile phone is turned on, the HLR will notify the SMSC and provides the correct MSC address to route the address. SMSC then delivers the message to MSC and MSC will send the message to indicated BSC by checking out the location of mobile equipment through local VLR. BTS will receive message from BSC and finally delivers the message to recipient's mobile phone.

Section 3. Wireless messaging protocols

Sneaking into the wires

In order to talk directly to the SMSC, the application must understand the protocol over which SMSC communicates, and a plethora of protocols exist made by the SMSC vendors. These are the protocols that handle data transfer over the wires in the form of packets, between an application or network component to SMSC. The vendor-specific protocols make the life of application developers uneasy, as they have to make customized changes in their application for different SMSC. Nevertheless some of the protocols that cover major market share are as follows:

- SMPP 3.4 by SMS Forum
- UCP/EMI 4.0 by CMG
- SMS2000 OIS 4.0 by Sema Group
- CIMD2 by Nokia
- TAP & SMTP

Short Message Peer to Peer (SMPP)

The SMS Forum is responsible to nurture the most popular SMS protocol. It is the widely accepted protocol that is used by major SMSC vendors and application softwares. Currently SMPP version 3.4 is used over the network, and many development toolkits are available to write programs that can understand this protocol. Using this interface, an external Short Message Entity such as a Paging or VoiceMail system may bind/unbind to the SMSC, submit, cancel, replace and query short messages. The SMSC forwards responses and short messages (e.g. delivery receipts, pager messages) to the external Short Message Entity.

Universal Computer Protocol (UCP)

European Telecommunication Standards Institute (ETSI) formally used the Universal Computer Protocol, or UCP for short, for paging networks. It is the strong competitor of SMPP in Western Europe, a place where SMS market is successful. UCP version 3.5 is nowadays used and supported by most SMSC vendors. An innovative trend will be provided along with UCP 4.0, in which content-based reverse charging can become possible, so its popularity is expected to rise sharply.

Open Interface Specifications (OIS)

The Open Interface Specification (OIS) was originated by Sema Group, now owned by Schlumberger. OIS is not so popular as SMPP or UCP, but it is as important as other protocols. This is because OIS is the only SMS application protocol that makes Vodafone networks accessible, the world's largest network of cellular communication. OIS version 5.1 is used nowadays that is supported by Schlumberger and CMG SMSCs.

Computer Interface to Message Distribution (CIMD)

The well-known Finnish-based company Nokia created the Computer-Interface to Message Distribution (CIMD2). It is used in very few networks and only on Nokia's SMSCs, but its importance is now diminishing because of Nokia SMSCs are now capable to understand SMPP and UCP.

Telocator Alphanumeric Protocol (TAP) and Simple Mail Transfer Protocol (SMTP)

American-originated protocol, the Telocator Alphanumeric Protocol (TAP) was originally used for two-way paging networks. Its importance is unique in a sense that it is used to interconnect SMS networks and the American paging networks, and porting the paging-powered applications to SMS networks. It is supposed to be a legacy system and does not support sending the ring tones, picture messages and so on. Not a good choice for the development of SMS applications.
The Internet Engineering Task Force (IETF) guys defined the SMTP and never thought that it can be used other than sending the emails, but many network providers are rolling the email addresses that are similar to the subscriber's phone number and any mail sent to that number can be received as a wireless message. Mostly the SMTP is used for sending the multi-media messages to the mobile phones, reading and posting the mails from the mobile phones.

Section 4. SMPP over TCP/IP

Out in the wild

Just like other Internet packets traveling across the networks, an SMPP packet can travel freely over IP networks and can be destined to an SMSC or SMS-powered application. Thanks to many Application Programming Interfaces (APIs) and toolkits, these unique packets can be created and sent to the wireless messaging networks by using computer networks. Thus TCP/IP can be used as an underlying protocol for the communication between an application and SMSC. Note that External Short Message Entity (ESME) refers to such external sources and sinks of short messages as Voice Processing Systems, WAP Proxy Servers or Message Handling computers. It specifically excludes SMEs, which are located within the Mobile Network, i.e., a mobile station (MS).

The general format of an SMPP PDU consists of a PDU header followed by a PDU body as outlined in the following table:

SMPP PDU				
PDU HEADER (MANDATORY)			PDU BODY (OPTIONAL)	
COMMAND LENGTH	COMMAND ID	COMMAND STATUS	SEQUENCE NUMBER	PDU BODY
4 OCTETS	LENGTH = (COMMAND LENGTH VALUE - 4) OCTETS			

PDU Header
The SMPP Header is a mandatory part of every SMPP PDU and must always be present.

PDU Body
The SMPP PDU Body is optional and may not be included with every SMPP PDU.

Command Length
Defines the total octet length of the SMPP PDU packet, including the length field. The Command Length field is 4 octets long.

Command ID
Identifies the particular SMPP PDU, e.g., submit_sm, query_sm, etc. The Command ID field is 4 octets long.

Command Status
Indicates the success or failure of an SMPP request. It is relevant only in the SMPP response PDU and it must contain a NULL value in an SMPP request PDU. The Command Status field is 4 octets long.

Sequence Number
Contains a sequence number that allows SMPP requests and responses to be associated for correlation purposes. The use of sequence numbers for message

correlation allows SMPP PDUs to be exchanged asynchronously. The Sequence Number field is 4 octets long.

Mandatory Parameters
Following the header is a set of mandatory parameters, corresponding to the SMPP PDU defined in the Command ID field.
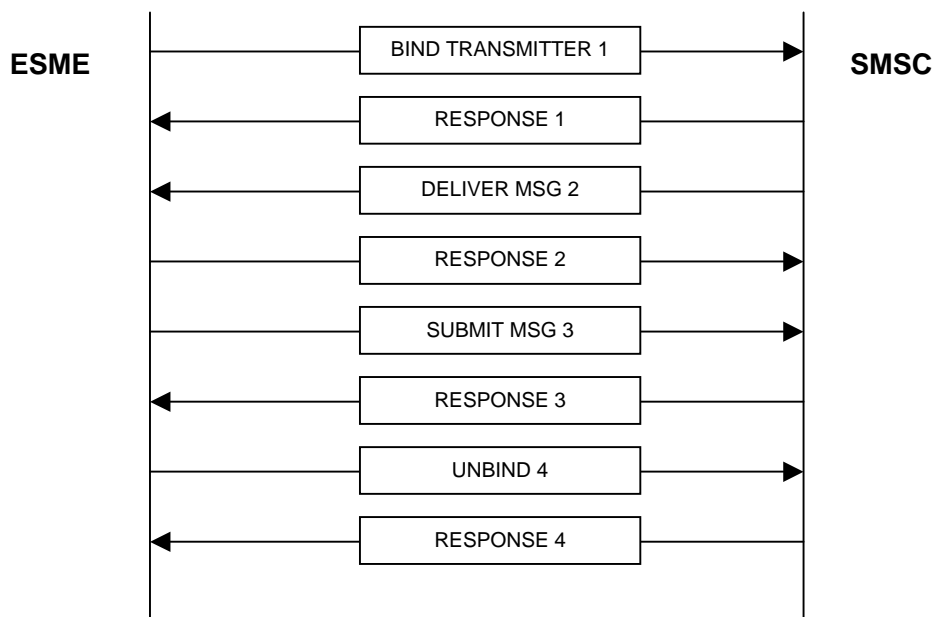
Optional Parameters
Optional parameters corresponding to the SMPP PDU defined in the Command ID field, and included as required.

Length
Indicates the length (in octets) of the Value field. The Length field is 2 octets long.

A Message Transfer Scenario (from ESME to SMSC)

ESME	BIND TRANSMITTER 1 →	**SMSC**
	← RESPONSE 1	
	← DELIVER MSG 2	
	RESPONSE 2 →	
	SUBMIT MSG 3 →	
	← RESPONSE 3	
	UNBIND 4 →	
	← RESPONSE 4	

The ESME first initiates a connection with SMSC in 'transmitter' mode (BIND TRANSMITTER 1). If the credentials submitted are valid, the SMSC will acknowledge the connection (RESPONSE 1). If the SMSC is free to serve the ESME, it generates the request to handover the message (DELIVER MSG 2). Upon receiving this signal, the ESME will acknowledge it (RESPONSE 2) and transfers the message along with recipient's necessary information (SUBMIT MSG 3). If the data transfer is successful, the SMSC will generate an acknowledgement to it (RESPONSE 3). If the ESME does not wish to send another message, it generates unbind request (UNBIND 4), which is granted by SMSC (RESPONSE 4), and the connection is closed.

Section 5. Current wireless messaging applications

Success stories

In general, wireless messaging applications can be categorized into three kinds of services; Information Services, Location-Based Services (LBS), Communication and Entertainment Services. These cover the major market share in real world today. Some of the most successful messaging services are described below:

- Citibank (Personal Alerts & Notifications)
- Shazam (Personal Alerts & Notifications)
- Jurong Point (LBS)
- KDDI (LBS & Remote Tracking)
- BattleMail (Entertainment)
- SMS2Email & IM (Communication & Entertainment)

Citialerts – Wireless Banking

Citibank Middle East provides its customers s service that can send alerts related to their spending habits and withdrawals, as well as the latest movements in the Stock Markets of the world. It is a service that provides customers flexibility to keep track of their bank accounts and receive the latest news and stock prices.

Shazam Entertainment – Song Tagging

Shazam has developed a real-time song identification service. Any sound track a customer hears can be identified by this service. A 15 second sound sample is fetched and send by the customer to Shazam via SMS, and within seconds a comprehensive reply can be received containing the name of the song and the artist, moreover information regarding how to purchase the album can also be sent.

Jurong Point – Location-Based Marketing

By identifying the nearest cell to the mobile phone, network operators can gain a rough idea where the customer is and that information is used to push information according to the surroundings of the recipients. In the above mentioned shopping center, the shoppers receive a series of short messages as long as they stay within the shopping area, concerning about the shop events and incentives in the shopping mall.

KDDI – In-Car Telemetry

Telematics deals with the route guidance is another Location-Based Service (LBS). The recipients of messages from this service are directed about shortest routes, traffic congestions ahead, GPS tracking and text based directions in guiding the drivers from unknown regions.

BattleMail – Mobile KungFu

A worldwide competition in which players can challenge one another to a virtual KungFu BattleMail, making moves using SMS to try to outwit their opponents with a series of high kicks and karate chops. This multiplayer fighting game achieved the heights of success. Since the launch, 25 million challenges and more than 20,000 fights have taken place across networks, boundaries, and nationalities.

SMS2Email & IM – Mobile Mailbox

Email is the killer app ion the Internet, and is now moving over the mobile networks. With the launch of services such as MSN Mobile Hotmail and i-mode, users can now entertain themselves with web-based email services over their mobile phones. Until 2003, more than 110 million Hotmail users were subscribed to their MSN Hotmail accounts on their mobile phones.

Instant Messaging (IM) is also another attractive service for 2-way instant communication and entertainment. It is merely a faster version of SMS or email; it also provides information like online status of the users.

Section 6. Developing SMS-powered applications

Many ways to skin a cat

Until now we have discussed the rich features of wireless messaging applications and their usage in commercial areas. Lets take a look at how these applications can be developed in real world and using the lowest possible set of resources.
The application development of SMS-powered application is categorized by handling the middleware architecture. The sole responsibility of handling wireless messages can be assigned to third-party vendor, a proprietary SMSC, or can be delivered to personally owned hardware.

Using the third-party

This is the most popular way to make SMS-powered applications. With some amount paid to the message vendors, you can relieve yourself from the pain to delivering the messages. A set of Application Programming Interface (API) is provided by the vendor, which is then implemented in your application software. Usually a socket-based Internet connection is established from the application and message servers. The contents are transferred via Internet from client side to the vendor server, it then moves forward to the wireless networks. Many third party vendors also provide 2-way messaging system.

Connecting to SMSC directly

The fastest way to transfer wireless messaging contents is the direct connection to the SMSC, but it includes many complexities. For example, the SMSC is exposed to any external connection, legal issues of using the provider resources, maximum connection capability of SMSC and authentication credentials floating over insecure connections. The communication link between SMSC and application software can be a TCP/IP network or an X.25 connection.

Use your own hardware

It is a cost effective way to implement lightweight applications within the complete administration of the application developer. Many hardware products are available that can act as an adapter between the TCP/IP network and wireless networks. For instance, a GSM modem connected to serial port of a computer can transfer data to and from GSM networks and pass it to application running on that computer. However the performance of GSM hardware can be a serious issue during heavy loads of data transfer.

Section 7. SMS vulnerability analysis

All about wareZ

With the advent of Multimedia Messaging Service (MMS) and SS7 over IP, core GSM network equipments are more exposed to the malicious attacks. These attacks can cause serious blow on Quality of Service (QoS), privacy and authenticity of subscribers, and disturbance in normal operations of life. Numerous vulnerabilities can be found in wireless messaging infrastructure and they can be categorized according to their environment. The most vulnerable places where the hackers of the future will likely compromise are:

- SMSC-Kernel.
- Connection between ESME and SMSC.
- Air interface of GSM.
- Network Equipments of GSM.
- Operating System of mobile phone.

Each category posses its own risk level and payload of the attack can devastate the whole of network. Until now, no such severe attacks were launched on the wireless messaging systems, but it is only a matter of time. Below is the discussion of most likely attacks that will occur in the future of wireless messaging systems.

Denial of Service (DOS) Attack

Most SMSCs are behind the firewall, but that greatly increases the network latency and delay in message transmission, so vendors do put SMSC exposed to DOS attacks for the sake of high performance. Nevertheless an improper configured firewall cannot protect an SMSC from DOS attacks, and talking about Distributed Denial of Service (DDOS), they are the most difficult to defend against.

Service Interruption Attack

Similar to DOS attacks, a Service Interruption Attack often occurs against a poorly tested platform, containing several security holes or 0-day exploits that can be used to compromise the target. Like the "WinNuke" vulnerability of 1997, which causes Windows 95 System to crash when it receives a specifically formatted TCP header, the SMSC can be on the target of such deliberately crafted SMPP packets to exploit the holes and bugs in the system.

Service Hijacking Attack

It relates to the gaining of control over the compromised target, what the hackers termed as access to 'root'. Service Hijacking involves unauthorized access to user that can cause change or loss of data on the system. This can involve message capturing, alteration of text and block of outgoing packets from the system.

Buffer Overflow Attack

It can be part of Service Hijacking Attack, to gain control over the box. Buffer Overflow occurs due to the uncheck bounds in the allocated memory, and that can cause arbitrary instructions to be executed on the target machine. The Buffer Overflow can be related to the SMSC kernel, the operating system underlying the SMSC, the database used by SMSC or the type of server used by the SMSC.

Password Compromise Attack

Social Hijacking and Brute Force technique can do a lot in this type of attack. If enough time is given, the password of SMSC can be detected using trial and error method. Once a password is guessed, it can cause severe blow to the messaging system. Another way to compromise password is "piggybacking". In this type of attack, a hacker first gains access to trusted machines by SMSC, normally a mail server. It then uses the compromised machine to drive the SMSC according to its will.

Snooping

Snooping or Sniffing, it can capture packets from the network through any kind of sniffer. The captured packets are decoded and they can give most valuable information. Many advanced sinffers like Ethereal, can capture SMPP packets along with the capability of tracing the handshakes during the whole session. This can give the idea what is going on between the ESME and the SMSC.

Spoofing

SMS packets can be created and injected in the network by using any ordinary packet creation utility, like Nessus that creates packets for TCP/IP network. Spoofing obfuscates the identity of the sender, and pretends that the message was originated form some other source. Just like there is no check in the current SMTP messages, a hacker can create a malicious control message under the disguise of trusted user and can compromise the network.

Radio Frequency Jamming

It is truly a non-Internet based attack that is related to the wireless interface of the communication system. Its sole purpose is to deny the service from being used by the subscribers in a particular area. The jamming equipment can be a noise-generating source that emits arbitrary signals in the frequency spectrum of GSM (normally 900 and 1800 MHz). It not only disrupts the SMS messages but voice calls can also be affected.

OSS Penetration

The most important part of a GSM network is actually not the Network Equipments themselves but the Operation and Support System (OSS) itself. It is a network of devices that manage important functions like billing system environment and those functions are very critical to the security of the GSM. Most interesting part of OSS is that this infrastructure is accessible via IP, so all the vulnerabilities in the network are inherited directly into OSS.

SMS Spam

Unwanted emails are havoc to any online organization. Similarly unsolicited electronic messages become a nuisance for users of wireless devices. If a wireless provider gets a block of several thousand subscribers, it can send bulk messages of all the recipients, causing unnecessary traffic load and disturbance to the recipients. Legal steps have been taken by some governments for spam protection over wireless, and investment has been done to develop anti-spam systems.

Mobile Virus

It is actually a bug in the mobile equipment software that can allow unauthorized access to programs or execution of instructions. Most SMS viruses ever noted can cause shutdown and crash of system software. Examples of other viruses are:

Palm.Phage.A:
A Malware affecting PalmOS can range from traditional viruses that infect executables to malicious code embedded in shared executables. Successful exploitations can range from device lockup to a low-level device wipe.

Cabir:
This worm spreads through a Bluetooth vector on supported platforms, and displays a warning about the unsigned code upon execution.

Dust:
This Malware demonstrates the potential for keystroke logging, remote device control, process hiding, and covert File Transport Protocol (FTP) server deployment in Windows CE Operating System.

Brador Trojan:
During the first week of August 2004, the first known Pocket PC virus/trojan utilizing some of the characteristics described in Dust was found in the wild. Two independent antivirus companies detected and analyzed samples of a backdoor process that can give an attacker complete control over a Pocket PC mobile device.

SMS Crash

Many text patterns are discovered that can be used to crash the recipient mobile equipment. The flaw lies not in the SMS packet format, but the operating system of the recipient mobile phone. News from BBC reported several hundreds of specific model equipment of a mobile phone crashed in Scandinavia upon receiving a unique pattern of SMS text message.

Section 8. Securing the message

"To the keep!"

Below is a short description of how to secure the wireless messaging applications.

Air Interface Algorithms

GSM level encryption must be enhanced that would be hard to break. Currently used Symmetric Algorithm encryption 'A5' provides radio communication ciphering, and has four levels of encryption. Recommended level is A5/3 (Note that A5/3 has been broken in 1999).

Proprietary Encryption

Proprietary encryption should be applied for intra-network communication and among network equipment. This kind of state of the art cryptographic technique is also necessary to keep the data transfer secure to and from ESME and SMSC.

Firewalls

SMSC and OSS should be behind well-configured firewalls and their network structure must be kept hidden from public network as far as it is possible. Modern IDS must be coupled with the network component to keep them safe from DOS Attacks and Network Scanning.

Secure Socket Layer

For the Internet and Transport layer, SSL and VPN should be used that can reduce the penetration threats. Moreover a white list of IP addresses should be maintained for the communication among allowed machines, with proper authentication.

AVs for the mobile?

Finally, to keep the mobile equipments safe from the malicious code, proper virus scanners should be installed with the mobile operating system, unsigned codes must be disabled.

Section 9. Conclusion

If you think it is secure, think again!

This sums up our discussion on wireless messaging protocols and applications, with the relevant threats faced by them. Although this is not a complete document, but it focuses the potential targets of the future panorama. The precautions and security measures can be applied to all level of the system, ranging from encrypted air interface to hiding the machines behind stateful firewalls and IDS dogwatch. More sensitive applications like bank account alerts and debit/credit card payment services must be ensured to keep the verification of the origin of message. No doubt that the network operators will eventually switch to IP networks in order to overcome bandwidth issues and multimedia messages, and that decision can open doors to many security threats that linger today due to isolated networks so far.

Wireless Messaging can be very effective medium of communication in the future. With new technologies like EMS, MMS, LBS, and VR technologies, its perspective can expand manifolds. The best thing about wireless messaging applications is that it can be developed with no or very little cost, and easy to implement. However, there is a strong requirement to improve security and authentication/authorization techniques in SMS based applications.

Section 10. References

[1] Donald J. Longueuil. *Wireless Messaging Demystified: SMS, EMS, MMS, IM, and others*. McGraw-Hill Professional Publishing, 2003

[2] The International Engineering Consortium.http://www.iec.net

[3] Kannel Userguide.http://www.kannel.org

[4] SMPP Protocol Sepcification.http://www.smsforum.com

[5] NetSec Mobile Computing Security Threats

[6] SMS over SS7, National Communication System.http://www.comtechnologies.com

[7] SMPP v3.4 Implementation Guide.http://www.smsforum.net

[8] GSM Association Official Documentation

[9] Toni Janveski. *Traffic Analysis and Design of Wireless IP Networks*. Artech House

[10] Ethereal Network Traffic Analyzer.http://www.ethereal.com