Exploiting Vulnerabilities and Security Mechanisms in Internet based SMS capable Cellular network

Akramul Azim[1] , Anwarul Azim[2], Tarikul Alam Khan Sabbir[3] ,Ashequl Qadir[4]
[1] Faculty of Comp. science & Information Tech., Islamic University of Technology, Bangladesh
[2] Jodrey School of Computer Science, Acadia University, Wolfville, Nova Scotia, Canada
[3] Engineer, Technical division, Banglalink , A subsidiary of ORASCOM Telecom Ltd.
[4] System Engineer, Technical division, Grammenphone Ltd

Abstract

Cellular networks are a very demandable component of the economic and social infrastructures in which we live. To give various latest technology services Telecommunication companies offer connections between their networks and the Internet. The Next generation Network (NGN) will be associated with the Internet. This leads to the cellular networks become more vulnerable because of some security holes. SMS capable cellular networks can be attacked by means of Spam, Spyware, Phishing, Viruses. Several prevention mechanisms can be applied but not adequate. In this paper these vulnerabilities are exploited and some mechanisms are proposed to alleviate the threats. It's a big challenge to handle these attacks as cellular network is becoming essential for the people.

Keywords
Cellular network, Open functionality, Channels, SMSCs, Internet.

1. Introduction

A Mobile network is a radio network made up of a number of radio cells each served by a fixed transmitter, known base station. These cells are used to cover different areas in order to provide radio coverage and this introduces Cellular connectivity. Cellular networks are inherently asymmetric with a set of fixed main transceivers each serving a cell and a set of distributed systems which provide services to the network's users. In this paper Mainly Denial of Service Attacks (DoS)Attacks through the Messaging Service and by the Mobile users is described. Also how to remedy from these attacks are described. This paper also describes several important issues that can make the cellular network vulnerable and also discusses several open research issues.

Manuscript received November 5, 2007
Manuscript revised November 20, 2007

2. SMS Capable Internet based Cellular network overview

With the inherent arrival of 3G (3rd generation) wireless communication systems mobile phone manufacturers and network operators are in search of features and services that will make use of the promised technological advances. They are also seeking to identify those solutions that will impress customer demand and boost waning sales of both mobile phone handsets and service contracts. Various possibilities have been suggested to meet these demands [3]. Multimedia messaging (MMS), for example, has been designed to extend the hugely popular short text messaging (SMS) facility, available on existing digital networks, by enabling users to exchange still images, sound and video content. GPRS, EDGE are the 2.5G and 2.75G Services that allows the connectivity of the cellular network with the Internet. Video conferencing, instant messaging, ticket reservation, online banking for example can be induced in the cellular network with the revolution of using the cellular phone. There are some External Short Messaging Entities by which SMS can be submitted to the SMSC via the Internet. Web Interfaces, High speed Modems are the examples. SMSC is short for "Short Message Service Center," and is the machine(s) within a Cellular network that provides the routing of all SMS or text messages. Much like an email server, the SMSC handles large volumes of messages sent to it. ESME includes several interfaces, equipments that are connected with the SMSC through the Internet. In terms SMSC(s) are connected with the Cellular network which consists of several MSC (Mobile switching centre)s, BSC(Base Station Controller)s, VLR(Visitor location register)s, HLR(Home location register)s and Other devices that establishes a Cellular network Architecture. By using ESME through Internet SMS can be sent to the cellular network via SMSC.

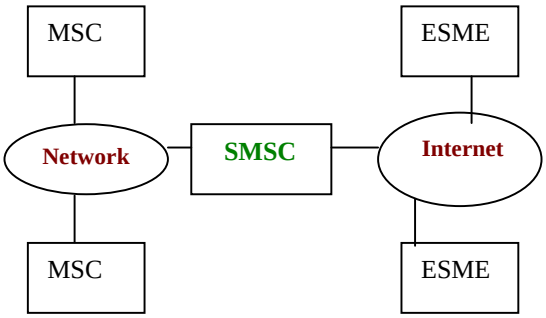

Fig: A simplified Architecture of the SMS capable Internet based Cellular Network (Base Station, Mobile Station, HLR, VLR and other devices of cellular network are not depicted because of simplification).

3. Vulnerability in Internet based Cellular network

One of the things that make attacks on Internet service more dangerous than attacks in the physical world is the automation that is possible in the world of computers. The worry is that in the physical world, attacks do not scale very well, but as soon as a physical world process is moved online, malicious parties can potentially exploit the vulnerabilities in an automated and exhaustive fashion. When the cellular network is involved with Internet then several kinds of Internet attacks can also launched in the cellular network because of the security holes.

3.1 Channels in the Cellular network

Air interface channel of cellular network is divided into Traffic Channels (TCHs) and Control channels (CCHs). The CCHs are intended to carry signaling information. Three types of CCHs are defined. These are Common control channels (CCCHs), Dedicated Control channels and the Broadcast channels (BCHs). Under the Common control channels there are paging channel, Access Grant channel, Random access channel. Paging channel is used by the network to page the destination MS in call termination. The MSs for initial access to the network uses access grant channel. Again, There are several dedicated control channels, which are Standalone dedicated control channel (SDCCH), Slow associated control channel (SACCH), Fast associated control channel (FACCH), Cell broadcast channel (CBCH). SDCCH is used only for signaling and for short messages. SACCH is used for transmission of power and time alignment control information over the downlink and measurement reports from the MS over the uplink. FACCH is used for time-critical signaling such as call establishing progress, authentication of subscriber or handoff. CBCH carries only the short message service cell broadcast messages. Broadcast channels are used by the BTS to broadcast information to the MSs in its coverage area. Traffic channels are used for the voice transmission. All of the details are described in [6]. These channels functionality can be used for inducing some threats in cellular network. Suppose, if channel jamming occurs by the adversary the call blocking will occur in the network.

3.2 Bottlenecks in the Cellular network

The bottlenecks described in [1] include the Delivery discipline, Delivery rate and Interfaces. Recognizing these bottlenecks requires a deeper understanding of the system.

3.2.1 Delivery Discipline

SMSCs are used for the SMS message flow. All messages pass through them. Each SMSC only queues a finite number of messages for each user. So, the buffer capacity and eviction policy determine which messages reach the recipient. As SMSCs route messages according to a store and forward mechanism, each message is held until either the target device receives it successfully. When the buffer saturates then all those messages will become lost after saturation. Not only SMSC Buffer but also MS Buffer limitation is also responsible for this kind of message loss. So for the reliable delivery a discipline rule should be maintained.

3.2.2 Delivery Rate

Delivery rate is the speed at which a collection of nodes (SMSC) can process and forward a message. It is possible to submit hundred or thousands of messages per second into a network from the Internet by using simple interfaces. If delivery rate exceeds then several messages will be lost as mismatch occurs in the data flow rate.

3.2.3 Interfaces

There are several interfaces by which attacks can be done by injecting large number of messages, which exceeds the network and phone capacity as well as the delivery rate. Interfaces can be grouped into three main categories: instant messaging, information services, and bulk SMS. Instant messaging supplies the same functionality as text messaging, but connects new networks of users to the cellular networks. By information service providers such as CNN and MSNBC, customers are frequently flooded with the updates of headlines, sports, and stocks. Lastly, by using bulk SMS providers,

companies can provide employees with updates ranging from server status to general office notifications.

3.3 Attack-list creation in the Cellular network

For launching successful DoS Attacks Hit list creation (A database of Potential targets) is necessary. Hit list can be created by NPA, Web Scraping, Web Interface Interaction, by taking information from recently called list, by taking information from hidden devices.

3.3.1 NPA

NPA means Numbering Planning Area. This information is useful to an attacker as it reduces the size of the domain to strictly numbers administered by wireless providers within a given region. This approach is extremely powerful when used in conjunction with other methods, as it reduces the amount of address space need to be explored and so that attacker gets a direction to do harm of the network.

3.3.2 Web Scraping

Web Scraping is a technique to collect information on potential targets commonly used by spammers. Through the use of snooping agent, scripting tools and search engines, these individuals are able to gather email addresses posted on web pages in an efficient, automated fashion. These same search tools can easily be harnessed to collect mobile phone numbers listed across the WebPages.

3.3.3 Web interface interaction

Several web interfaces are established for sending the SMS. When a person submits a message then he/she also needs to provide the Cell number. If that kind of interface is linked with the Hit-list creation database then the cell numbers are stored in the database. By using this technique it can be possible to collect large number of cell numbers.

3.3.4 Taking information from Recently called list

A worm could be designed to collect stored mobile phone numbers from victim devices by address book scraping. In order to increase the likelihood that a list contained only valid mobile phone numbers, the worm could instead be programmed to take only the numbers from the “Recently Called” list.

3.3.5 Taking information from Hidden devices

Bluetooth enabled devices have become dangerous for leaking information. In a busy area such as a bus, subway or train terminal, a Hidden device designed to collect this sort of information through continuous polling of Bluetooth enabled mobile phones in the vicinity would quickly be able to create a large hit-list that can be attacked.

3.4 Bandwidth Requirements to Saturate

The wireless portion of SMS delivery starts when the targeted device hears its Temporary Mobile Subscriber ID (TMSI) over the Paging Channel (PCH). The phone acknowledges the request through the Random Access Channel (RACH) and then proceeds with authentication and content delivery over a Standalone Dedicated Control Channel (SDCCH). Voice call establishment is very alike to SMS delivery, except a Traffic Channel (TCH) is allocated for voice traffic at the completion of control signaling. The total number of SDCCHs available in a area is typically depends upon the location/population density. In Urban area 8 SDCCH, In rural area 4 SDCCH, Densely populated metropolitan area may have 12 SDCCHs.

$$\text{Capacity} = (N)\left(\frac{S}{1}\right)\left(\frac{\text{SDCCH Capacity}}{1}\right)$$

Where

N= Number of Sectors
S= Number of SDCCHs

The bandwidth needed to induce saturation depends upon the Capacity, which indicates the number of messages per second. The adversary’s bandwidth requirements can be reduced if the single message is repeated to several recipients. For example, if the same message is intended for 10 recipients then the upload bandwidth is reduced by factor 10 as the message need to be uploaded at the SMSC one time. But if it is not same then need to upload the message 10 times.

3.5 Common Internet Attacks

There are several Internet attacks that are described in [2,4,5]. Among then Spamming, Phishing, Spyware, viruses are the common attacks that can be easily launched in Internet based SMS Capable Cellular network. Several prevention mechanisms also exist but those are not adequate to assure the full protected operating system. The

following sections describe the details of these attacks in the aspect of these network.

3.5.1 Spam

Spam is Unwanted, unsolicited email. Spam refers to electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. In addition to being a nuisance, spam also eats up a lot of network bandwidth. Because the Internet is a public network, little can be done to prevent spam, just as it is impossible to prevent junk mail. However, the use of software filters in e-mail programs can be used to remove most spam sent through e-mail.

3.5.2 Phishing

Phishing is the act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn't do or shouldn't do. For example: sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. As cellular network is connected with the internet so this kind of attack can easily be launched by sending email to the Mobile Station. Authentication software can be installed at the Mobile Station side for protecting Phishing.

3.5.3 Spyware

Spyware gathers user information through the user's Internet connection without his or her knowledge usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. This kind of attack can also be launched to the Mobile Station. Every mobile station should have the facility to block such kind of Spyware so that it cannot be downloaded.

3.5.4 Viruses

A virus is a program or code that attaches itself to a legitimate, executable program, and then reproduces itself when that program is run. Worm: A self-contained program (or set of programs) that is able to spread copies of itself to other computer systems. Usually takes place through network connections or email attachments. Trojan Program: A program that neither replicates nor copies itself, but performs some illicit activity when it is run. Viruses can easily come through the email attachment via the SMSC. And as Mobile terminal has not lot of processing power so it can be easily attacked. Several antiviruses should be designed that are capable of protecting the attacks.

3.5.5 Attack Sources

These attacks can be generated through High end cable Modem, Zombie Network (Using some Valid IP address for Attacking) and Several Web Interfaces. These sources can also passes some agents, which cause the disruption of the Cellular network. The agents can be sent through the email attachment or via downloading some software from the Internet.

3.5.6 Solutions

Several Solutions exists but those are not adequate. The possible solutions are Authentication based system. Limiting the maximum number of message received by an individual user and restricts access to SMS Messaging, Separation of Voice and Data Resource Provisioning, Rate limitation, All web interfaces should cease that are used for SMS submission, Remove the ability of Automatic SMS submission through interfaces, Close the interface between Web and cellular networks, Education so that people don't install anything without any judgment comes from the Network. So, before doing anything one must know what he/she is doing.

4. Conclusion

Security in Internet based SMS capable cellular network is an important issue of current world. Several terminologies of this paper like Spam, Spyware, Viruses etc are known to us but In these paper those terminologies are discussed in terms of Internet based SMS capable Cellular network. Due to the tremendous earnings potential associated with this Internet based SMS capability; it is also difficult to encourage service providers to restrict access to SMS messaging. If DoS Attacks happens in Cellular network then the companies will face a great loss. Now a days as Internet is involved so, the adversary can easily diminish the cellular network. As service providers never stop to give Internet based service so the NGN security is becoming a challenging Issue and researches should be done that includes all kind of protection by which the network can be much more secured.

References

[1] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta: Exploiting Open Functionality in SMS Capable Cellular Networks. CCS'05, November 7–11, 2005, Alexandria, Virginia, USA. Copyright 2005 ACM 1595932267/05/0011.
[2] S. Bellovin. Inside risks: Spamming, phishing, authentication, and privacy. Communications of the ACM, 47(12):144, December 2004.
[3] S. Berg, A. Taylor, and R. Harper. Mobile phones for the next generation: Device designs for teenagers. In Proceedings ACM SIGCHI Conference on Human Factors in Computing Systems, pages 433–440, 2003.
[4] S. Byers, A. Rubin, and D. Kormann. Defending against an internet-based attack on the physical world. ACM Transactions on Internet Technology (TOIT), 4(3):239–254, August 2004.
[5] Magda El Zarki, Sharad Mehrotra, Gene Tsudik and Nalini Venkatasubramanian: Security Issues in a Future Vehicular Network. European Wireless, 2002.
[6] Wireless & Mobile Network Architectures Author: Yi bing Lin, Page: 138-140.

Akramul Azim has received an undergraduate degree in Computer Science and Information Technology from Islamic University of Technology (an organization of OIC), Bangladesh. He worked in Huawei Technologies, a Telecom vendor company. Now he is a Lecturer of computer science and information technology department of Islamic University of Technology, Bangladesh. His research interest includes Wireless sensor networks, wireless adhoc networks, distributed systems. He has also strong interest on the security, mobility management and resource reservation in mobile networks.

Anwarul Azim has received an undergraduate degree in Computer Science and information Technology from Islamic University of Technology, Bangladesh. He is now doing his M.Sc in computer science from Acadia University, Canada. His research interest includes wireless sensor network, Wireless mesh network in radio harsh environment. He has also strong interest on cellular network.

Tarikul Alam Khan Sabbir received an undergraduate degree in Computer Science and Information Technology from IUT (Islamic University of Technology) from Bangladesh. He is currently working in telecom Industry as an Engineer in Banglalink (a Subsidiary of ORASCOM Telecom Ltd.), Bangladesh. His research interest focuses on Potential security threats and their possible solution in several Computer based networks or Mobile adhoc networks Such as Wireless Sensor Networks, Cellular Networks. He has a special liking in the field of Mobile computing and exploiting and enhancing the security measures in it.

Ashequl Qadir has received an undergraduate degree in Computer Science and Information Technology from Islamic University of Technology, Bangladesh. He has worked in the development project of Banglapedia (Digital version), Encyclopedia of Bangladesh. His research interest lies in Mobile Communication and Natural Language Processing. He currently works at Grameenphone Ltd. as a system engineer.