SMS ATTACKS AND SECURITY IN MOBILE COMPUTING

N.Janani
Dept. Computer Science & Engineering,
Karpagam College Of Engineering (KCE)
Coimbatore, TamilNadu, India
Email: blackmoon318@gmail.com

ABSTRACT: Cellular networks are a critical component of the economic and social infrastructures in which we live. In addition to voice services, these networks deliver alphanumeric text messages to the vast majority of wireless subscribers. To encourage the expansion of this new service, telecommunications companies offer connections between their networks and the Internet. The ramifications of such connections, however, have not been fully recognized. In this paper, we evaluate the security impact of the SMS interface on the availability of the cellular phone network.

The analysis begins with an exploration of the structure of cellular networks. We then characterize network behaviour and explore a number of reconnaissance techniques aimed at effectively targeting attacks on these systems. This paper describes in detail about the vulnerabilities due to DOS (Denial of Services) attacks. The major problem seen in this method is overflow of the buffer. To overcome the above problem, we have proposed a new idea of Weighted Fair Queuing. We conclude by discussing countermeasure that mitigate or eliminate the threats introduced by these attacks.

Keywords: *DOS attacks, Weighted Fair Queuing, Hit Lists, Overflow of buffer.*

INTRODUCTION

With digitalization the difference between telecommunication and computer net-working is fading and the same technologies are used in both fields. However, the convergence does not progress as rapidly as expected. Moving applications and services from one field to the other has proven to be very difficult or in many cases impossible. The explanation is that although the technologies in use are rather similar there are crucial differences in architecture and concepts. One of the major utility offered by the mobile services is the Short Message Service [1]. This has prone to a lot of vulnerabilities at present making the security very critical [2]. This paper mainly focuses elaborately about the SMS hacking and security.

Nowadays, In addition to traditional voice communications, cellular systems offer a wide variety of data and text/short messaging services (SMS). Cellular providers have introduced SMS gateways between the phone networks and the Internet to increase the reach (and volume) of text messaging. These gateways are partially responsible for the soaring usage of text messaging [3]. The migrating problem now-a-days arise due to DoS attacks [4]. Indeed, for significant numbers of users, text messaging has become the primary means of communication.

2. SMS / CELLULAR NETWORK OVERVIEW IN GSM TECHNOLOGY

This section offers a simplified view of an SMS message traversing a GSM-based system from submission to delivery. These procedures are similar in other cellular networks including CDMA.

2.1 Submitting a Message

There are two methods of sending a text message to a mobile device - via another mobile device or through a variety of External Short Messaging Entities (ESMEs). ESMEs include a large number of diverse devices and interfaces ranging from email and web-based messaging portals at service provider websites to voice mail services, paging systems and software applications. Whether these systems connect to the mobile phone network via the Internet or specific dedicated channels, messages are first delivered to a server that handles SMS traffic known as the Short Messaging Service Center (SMSC). A service provider supporting text messaging must have at least one SMSC in their network. Due to the rising popularity of this service, however, it is becoming increasingly common for service providers to support multiple SMSCs in order to increase capacity. Upon receiving a message, the contents of incoming packets are examined and, if necessary, converted and copied into SMS message format. At this point in the system, messages from the Internet become indistinguishable from those that originated from mobile phones. Messages are then placed into an SMSC queue for forwarding.

2.2 Wireless Delivery

The air interface is divided into two parts - the **Control Channels (CCH) and Traffic Channels (TCH).** The CCH is further divided into two types of channels - the Common CCH and Dedicated CCHs.

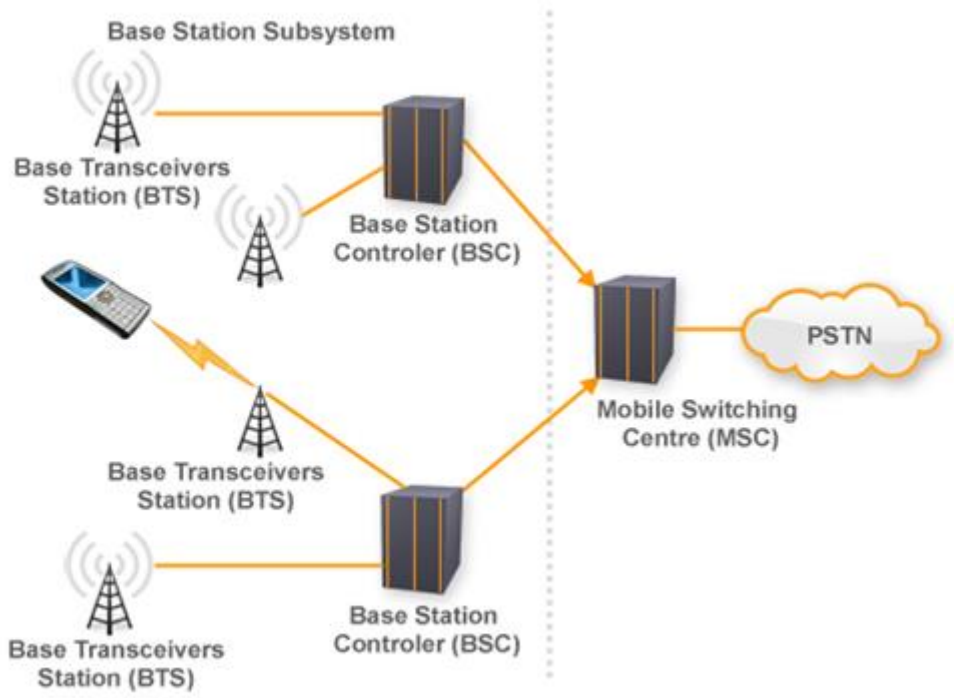

Base Station Subsystem
Base Transceivers Station (BTS)
Base Station Controler (BSC)
PSTN
Mobile Switching Centre (MSC)
Base Transceivers Station (BTS)
Base Station Controler (BSC)
Base Transceivers Station (BTS)

Figure 1: Simplified examples of an SMS Network

The Common CCH, which consists of logical channels including the Paging Channel (PCH) and Random Access Channel (RACH), is the mechanism used by the base station to initiate the delivery of voice and SMS data. Accordingly, all connected mobile devices are constantly listening to the Common CCH for voice and SMS signaling. The base station sends a message on the PCH containing Temporary Mobile Subscriber ID (TMSI) associated with the end destination. The network uses the TMSI instead of the targeted device's phone number in order to thwart eavesdroppers attempting to determine the identity of the receiving phone. When a device hears its TMSI, it attempts to contact the base station over the RACH and alerts the network of its availability to receive incoming call or text data1.

When the response arrives, the base station instructs the targeted device to listen to a specific Standalone Dedicated Control Channel (SDCCH). Using the SDCCH, the base station is able to facilitate authentication of the destination device (via the subscriber information at the MSC), enable encryption, deliver a fresh TMSI and then deliver the SMS message itself. In order to reduce overhead, if multiple SMS messages exist on the SMSC, more than one message may be transmitted over an SDCCH session. If a voice call had been waiting at the base station instead of a text message, all of the above channels would have been used in the same manner to establish a connection on a traffic channel.

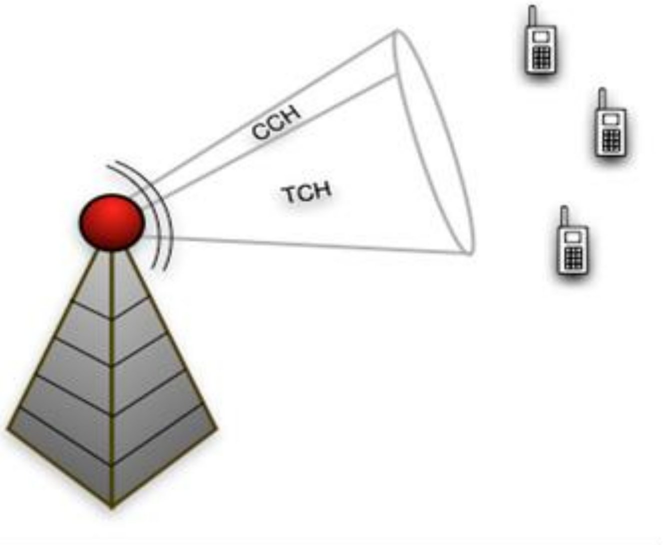


Figure 1(a): Simplified examples of a message flow.

3. SMS/CELLULAR NETWORK

VULNERABILITY ANALYSIS

We first characterize the systems through an extensive study of the available standards documentation and gray-box testing. From this data, we discuss a number of attacks and the susceptibility of mobile phone networks to each. Lastly, from gray-box testing, we assess the resilience of these networks to these attacks. Before discussing the specifics of any attack on cellular networks, it is necessary to examine these systems from an adversary's perspective. In this section, we present simple methods of discovering the most fragile portions of these networks by determining system bottlenecks. We then investigate the creation of effective targeting systems designed to exploit these choke points.

3.1 Determining Bottlenecks in Cellular Networks

There is an inherent cost imbalance between injecting SMS messages into the phone network and delivering messages to a mobile user. Such imbalances are the root of DoS attacks. Recognizing these bottlenecks requires a thorough understanding of the system. The cellular network standards documentation provides the framework from which the system is built, but it lacks implementation specific details. In an effort to bridge this gap, we performed gray-box testing.

We characterize these systems by delivery disciplines, delivery rates, and interfaces. All tests were performed using our own phones. At no time did we inject a damaging volume of packets into the system or violate any service agreement.

3.1.1 Delivery Discipline

The delivery discipline of a network dictates the way messages move through the system. By studying this flow, we determine system response to an influx of text messages. The buffer capacity and eviction policy therefore determine which messages reach the recipient. The SMSC buffer and eviction policy were evaluated by slowly injecting messages while the target device was powered off. Three of the most prominent service providers were evaluated: AT&T (now part of Cingular), Verizon, and Sprint. For each provider, 400 messages were serially injected at a rate of approximately one per 60 seconds. When the device was reconnected to the network, the range of the attached sequence numbers indicated both buffer size and queue eviction policy. We found that AT&T's SMSC buffered the entire 400 messages. While seemingly large, 400

160-byte messages are only 62.5KB. Tests of Verizon's SMSC yielded different results. When the device was turned on, the first message downloaded was not sequence number one; instead the first 300 messages were missing. This demonstrates that Verizon's SMSC has a buffer capacity of 100 messages and a FIFO eviction policy. Sprint's SMSC proved different than both AT&T and Verizon. Upon reconnecting the device to the network, we found only 30 messages starting with message number one. Therefore, Sprint's SMSC has a message capacity of 30 messages and a LIFO eviction policy.

Device Capacity (number of messages)

Nokia	3560 30
LG	4400 50
Treo	650 500*

Where,

* 500 messages depleted a full battery.

Table 1: Mobile Device SMS Capacity

3.2 Hit List Creation

The ability to launch a successful assault on a mobile phone network requires the attacker to do more than simply attempt to send text messages to every possible phone number. Much like the creation of hit-lists for accelerated worm propagation across the Internet, it is possible to efficiently create a database of potential targets within a cellular phone network.

3.2.1 NPA/NXX

The United States, Canada, and 18 other nations throughout the Caribbean adhere to the North American Numbering Plan (NANP) for telephone number formatting. NANP phone numbers consist of ten digits, which are traditionally represented as "NPA-NXXXXXX4". These digit groupings represent the area code or Numbering Plan Area, exchange code5, and terminal number, respectively.

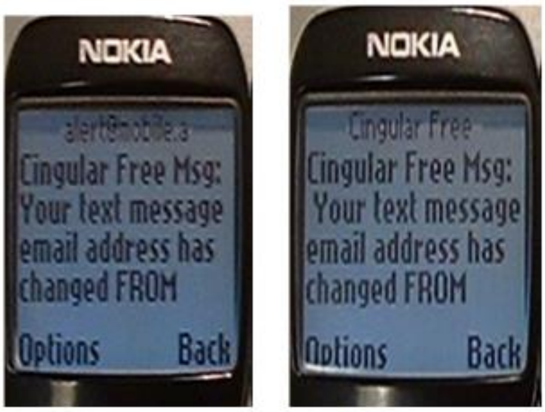
Traditionally, all of the terminal numbers for a given NPA/ NXX prefix are administered by a single service provider. A quick search of the Internet yields a number of websites with access to the NPA/NXX database. Responses to queries include the name of the service provider administering that NPA/NXX domain, the city where that domain is located and the subdivision of NPA/NXX domains among a number of providers. For example, in the greater State College, PA region, 814-876-XXXX is owned by AT&T Wireless; 814-404-XXXX is managed by Verizon Wireless; 814-769-XXXX is supervised by Sprint PCS. 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; however, this data does not give specific information in regards to which of the terminals within the NPA/NXX have been activated.

3.2.2 Web Scraping

As observed in the Internet, a large number of messages sent to so-called "dark address space" is a strong indicator that an attack is in progress. A more refined use of domain data, however, is readily available. Web Scraping is a technique commonly used by spammers to collect information on potential targets. Through the use of search engines and scripting tools, 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 web. For example, the query Cell 999-999-0000.9999 at Google (www.google.com) yields a large number of hits for the entire range of the NPA/NXX "999-999-XXXX".

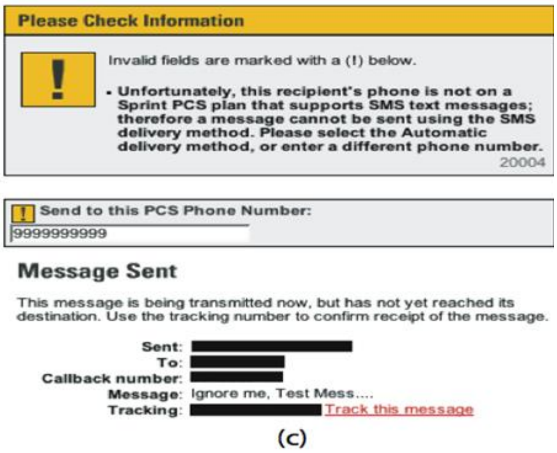
3.2.3 Web Interface Interaction

The message is sent to the targeted mobile device and a positive acknowledgment & a negative acknowledgment is delivered to the sender. An example of the both the positive and negative acknowledgments are available in Figure 3. Of the service providers tested (AT&T Wireless, Cingular, Nextel, Sprint PCS, T-Mobile and Verizon Wireless), only AT&T did not respond with a positive or negative acknowledgment; however, it should be noted that subscribers of AT&T Wireless are slowly being transitioned over to Cingular due to its recent acquisition. The positive and negative acknowledgments can be used to create an extremely accurate hit-list for a given NPA/NXX domain. Every positive response generated by the system identifies a potential future target. Negative responses can be interpreted in multiple ways. For example, if the number corresponding to a negative response was found through web scraping, it may instead be tried again at another provider's website.


alert@mobile.a
Cingular Free Msg: Your text message email address has changed FROM

Cingular Free
Cingular Free Msg: Your text message email address has changed FROM

Fig 2: Spoofing a service provider notification is trivial due to interface and message length constraints; the left image is a forgery of a legitimate service notification (right) provided by Cingular (Note the top line).


Please Check Information

Invalid fields are marked with a (!) below.

- **Unfortunately, this recipient's phone is not on a Sprint PCS plan that supports SMS text messages; therefore a message cannot be sent using the SMS delivery method. Please select the Automatic delivery method, or enter a different phone number.** 20004

Send to this PCS Phone Number: 9999999999

Message Sent

This message is being transmitted now, but has not yet reached its destination. Use the tracking number to confirm receipt of the message.

Sent: [redacted]
To: [redacted]
Callback number: [redacted]
Message: Ignore me, Test Mess....
Tracking: [redacted] Track this message

Fig: 3 Acknowledgments

4. MODELING DOS ATTACKS

Given the existing bottlenecks and the ability to create hit-lists, we now discuss attacks against cellular networks. An adversary can mount an attack by simultaneously sending messages through the numerous available portals into the SMS network. The resulting aggregate load saturates the control channels thereby blocking legitimate voice and SMS communication. Depending on the size of the attack, the use of these services can be denied for targets ranging in size from major metropolitan areas to entire continents.

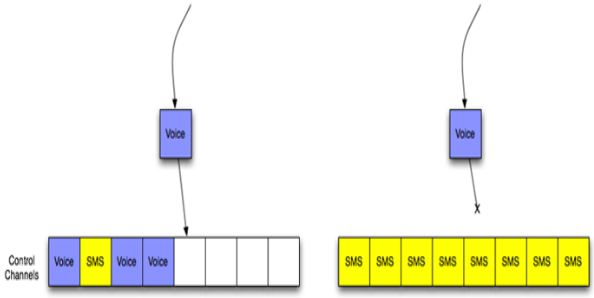


Figure 4: On the left, a request to set up a voice call is sent to the control channels. Because a number of unused control channels are available, the call will be connected. On the right, the control channels have been filled by SMS messages. If the attacker sends enough SMS messages to this particular tower, they can ensure that voice calls will always be blocked with a very high probability.

4.1 Targeted Attacks

While total network degradation attacks can occur, Internet attacks can be targeted. This same attack can be applied to SMS service. While the complete disruption of a user's SMS service is dangerous, a more interesting attack occurs when the adversary wishes to stop a victim from receiving useful messages. For example, a jealous ex-lover may wish to keep a message from being delivered; an attacker may want to keep a systems administrator from receiving a notification. This attack is accomplished by flooding the user with a superfluous number of messages. This result in one of three outcomes: a buffer somewhere overflows and the message is lost. Once the phone can no longer receive messages, the service provider's network begins to buffers all subsequent messages.

For reasons of practicality, providers impose limitations on the number of messages the network can store per user. Thus, if the adversary can exceed this value, messages become lost. The SMSC is not the only locus for message loss. As observed with the Nokia 3560, when the buffer became full, any message with content assumed to be known (any outbox message and read messages in the inbox) were automatically deleted. While this occurrence was isolated to the firmware of a specific phone, the potential to remotely maliciously destroy a user's data exists. Temporally critical messages were potentially delayed beyond their period of usefulness. Thus there exists a DoS attack.

6. SOLUTIONS

Many of the mechanisms currently in place are not adequate to protect these networks. The proven practicality of address spoofing or distributed attacks via zombie networks makes the use of authentication based upon source IP addresses an ineffective solution. The mechanisms below offer both long term and temporary options for securing cellular networks.

6.1 Separation of Voice and Data

In light of this, the most effective means of eliminating the above attacks is by separating all voice and data communications.

This separation should occur in both the wired network and at the air interface. Dedicating a carrier on the air interface for data signaling and delivery eliminates an attacker's ability to take down voice communications. Dedicated data channels, however, is an inefficient use of spectrum and are therefore unattractive. More importantly; separating text messaging traffic onto IP or dedicated SS7 links does not prevent an attack from overloading the air interface. Until offloading schemes are fully implemented in these networks, overload controls based upon origin priority should be implemented to help shape traffic. A partial separation has already begun with the introduction of data services including GRPS and EDGE; however, these networks will remain vulnerable to attack as long as Internet-originated text messages exist. The separation of voice and data is not enough to completely ensure unaffected wireless communications Text messages originating outside of the network should be assigned low priority on data channels. Messages originating within the phone network should receive high priority. This solution assumes that the SMSC is sufficiently protected from physical compromise by an attacker. If this expectation does not hold, more sophisticated, distributed mechanisms will have to be employed throughout the SS7 network.

6.2 Rate Limitation

Due to the time and money required to realize the above solutions, it is necessary to provide short term means of securing cellular networks. These techniques harness well-known rate limitation mechanisms. On the air interface, the number of SDCCH channels allowed to deliver text messages could be restricted. Given the addition of normal traffic filling control channels, this attack would still be effective in denying service to all but a few individuals.

Additionally, this approach slows the rate that legitimate text messages can be delivered, potentially elevating congestion in the core of the phone network. This approach is therefore not an adequate solution on its own. Because many of these attacks are heavily reliant upon accurately constructed hit-lists, impeding their creation should be of the highest priority. Specifically, all of the web interfaces should cease returning both positive and negative acknowledgments for submitted SMS messages. Instead, a message indicating only that the submission was being processed should be returned so as to not permit an attacker from accurately mapping an NPA/NXX domain. This is currently the behavior seen when a mobile-to-mobile message is sent.

Wireless websites is particularly dangerous as flooding the system requires one-tenth of the messages and bandwidth necessary to interfere with other networks.

6.2.1. PROPOSED IDEA

Because we cannot rely on rate limitation at the source of messages, we now explore network-based solutions. **Fair Queueing** is a scheduling algorithm that separates flows into individual queues and then apportions bandwidth equally between them. Designed to emulate bit-wise interleaving, Fair Queueing services queues in a round-robin fashion. Packets are transmitted when their calculated interleaved finishing time is the shortest. Building priority into such a system is a simple task of assigning weights to flows, Known as **Weighted Fair Queueing (WFQ**), this technique can be used to give incoming voice calls priority over SMS.

6.3 Education

While the above mechanisms are appropriate for the prevention of DoS attacks, they have limited success preventing phishing scams. Phishers will still be able to send messages to individuals through the web interface with anonymity; however, their ability to blanket large prefixes in a short period of time is greatly reduced. Unfortunately, it may only require a single message for an attacker to get the sensitive information they seek. Additionally, viruses will still be able to damage mobile devices as their introduction to a specific system is frequently the result of some user action.

The only practical solution for this family of exploits is therefore education. Cellular service providers must launch an aggressive campaign to reach all of their clients to tell them that no such request for information will ever come via SMS text. To this date, we are unaware of any such effort.

7. CONCLUSION

Cellular networks are a critical part of the economic and social infrastructures in which we live. The attacks discussed throughout are representative of growing and increasingly problematic class of vulnerabilities. The connectivity between the Internet and traditional voice networks introduces new avenues for exploit: once confined to exploiting only inert hosts, remote adversaries can debilitate the services we depend on to carry on our daily lives. In a broader sense, the ability to control the physical world via the Internet is inherently dangerous, and more so when the affected components are part of critical infrastructure. This work provides some preliminary solutions and analysis for these vulnerabilities. Essential future work will seek more general solutions that address these vulnerabilities in current and next generation networks.

8. REFERENCES

1. Exploiting open functionality SMS networks. (1)Thomas La Porta, (2) Patrick McDaniel. “Systems and Internet Infrastructure Security Laboratory - Department of Computer Science and Engineering”, Pennsylvania State University.

2. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. (1)Patrick Traynor, (2) William Enck. “Systems and Internet Infrastructure Security Laboratory - Department of Computer Science and Engineering”, Pennsylvania State University.

3. Networking and Security Research Center. G. Goth. “Phishing attacks rising, but dollars losses down”. IEEE Security and Privacy Magazine, January 2005.

4. P. Roberts, “Nokia phones vulnerable to dos attack”. (http://www.infoworld.com/), February, 2003.