Emergency Alert System using Android

L.Hariprasath[1], R.Dhivya[2], S.Adithya[3]

[1]Assistant professor, Department of IT, Anand Institute of Higher Technology
Kazhipattur, Chennai, Tamilnadu, India

[2&3]UG-Student, Department of IT, Anand Institute of Higher Technology
Kazhipattur, Chennai, Tamilnadu, India

Abstract

Emergency alert system alerts (EAS) people by sending text messages which third party cellular providers could not implement with the existing cellular infrastructure during the emergencies. Unfortunately, bulk messages cannot be sent during emergencies due to network traffic. This leads to denial-of-service (DoS) attack. EAS adapts certain mathematical techniques through which the bulk messages are split to avoid network congestion. These techniques are useful in finding the minimum time for the delivery of all messages. In this paper, the user can send an alert message to wide range of people in the organizations including colleges and universities. The EAS provides better security which does not wend way to intruders/hackers to take over the authority of the system. With the first five digits of the recipients' phone number the system is capable of generating the ten digit number series.

Index Terms—*SMS, campus alert, denial of service, security.*

1 INTRODUCTION

Cellular text messaging services are increasingly being relied upon to disseminate critical information during emergencies. Whether to coordinate meetings, catch up on gossip, offer reminders of an event or even vote for a contestant on a television game show, this discreet form of communication is now the dominant service offered by cellular networks. While many of the applications of this service can be considered noncritical, the use of text messaging during emergency events has proven to be far more utilitarian.

However, with voice-based phone services being almost entirely unavailable, SMS messages were still successfully received in even the most congested regions because the control channels responsible for their delivery remained available. Text messaging allowed the lines of communication to remain open for many individuals in need, in spite of their inability to complete voice calls in areas where the equipment was not damaged and power was available. SMS messaging is now viewed by many as a reliable method of communication when all other means appear unavailable.

Android is a software stack for mobile devices that includes an operating system, middleware and key applications. Google Inc. purchased the initial developer of the software, Android Inc., in 2005. Android's mobile operating system is based on the Linux kernel. Google and other members of the Open Handset Alliance collaborated on Android's development and release[1]. The Android Open Source Project is tasked with the maintenance and further development of Android. The Android operating system is the world's best-selling Smartphone platform.

The Android SDK provides the tools and APIs necessary to begin developing applications Android platform using the Java programming language. Android has a large community of developers writing applications ("apps") that extend the functionality of the devices. There are currently over 250,000 apps available for Android. It relies on Linux version 2.6 for core system services such as security, memory management, process management, network stack, and driver model. Android is an operating system based on Linux with a Java programming interface.

In this paper, we explore the limitations of third-party Emergency Alert Systems (EAS). This identifies a key failure in sending bulk messages during critical security incident response and recovery mechanism and demonstrates its inability in third party interaction.

1.1 EMERGENCY ALERT SYSTEM

The Emergency Alert System (EAS) is a media communications-based alerting system that is designed to transmit emergency alerts and warnings. EAS Participants broadcast thousands of alerts and warnings to the public each year regarding weather threats, child abductions, and many other types of emergencies. As such, the EAS will continue to function as one key component of a national alert and warning system that will provide alerts over multiple communications platforms, including mobile communications devices. The EAS alerting architecture is frequently used by state and local emergency managers to send alerts to the public about emergencies and weather events. Ensuring that the EAS architecture functions properly will benefit emergency alerting at all levels of government.

The EAS provides the ability to send messages regionally or nationally, though it has never been activated at these levels. But a major disaster like an earthquake or tsunami could necessitate the use of the EAS on a regional or national basis to send life-saving information to the public. We cannot anticipate which communications infrastructure will withstand a particular disaster, but the EAS is one of the tools we have to send alerts, warnings, and information to the people. The EAS can provide message receipt date, message receipt time and local time zone.

1.2 EMERGENCY EVENT CHARACTERIZATION

Through modelling and simulation based on real provider deployments, we provide the first public characterization of the impact of an emergency event on a cellular network. This contribution is novel in that it explores a range of realistic emergency scenarios and provides a better understanding of their failure modes.

1.3 MEASURE EAS OVER SMS FOR MULTIPLE EMERGENCY SCENARIOS

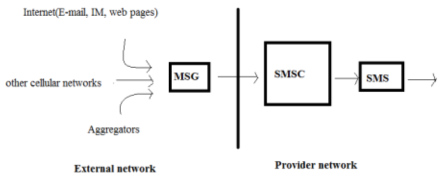
We provide data to debunk the common
Assertion made by many third-party vendors that large quantity of text messages can be delivered within a short period of time (i.e., seconds to minutes). We evaluate a number of different, realistic emergency scenarios and explain why a number of college campuses have reported “successful” tests of their systems. Finally, we provide a real world example that very closely mirrors the results of our simulations.

2 NETWORK ARCHITECTURE

Characterizing the cellular infrastructure during an emergency is necessary to understand how such networks deliver text messages. We specifically examine GSM networks in these discussions as they represent the most widely deployed cellular technology in the world; however, it should be noted that message delivery for other technologies such as CDMA,
IDEN and TDMA are very similar and are therefore subject to similar problems.

2.1 CELLULAR NETWORK ARCHITECTURE

There are a number of ways in which text messages can be injected into a GSM or CDMA network. While most users are only familiar with sending a text message from their phone, known as Mobile Originated SMS (MO-SMS), service providers offer an expanding set of interfaces through which messages can be sent. From the Internet, for instance, it is possible to send text messages to mobile devices through a number of web pages, e-mail, and even instant messaging software. Third parties can also access the network using so-called SMS Aggregators. These servers, which can be connected directly to the phone network or communicate via the Internet, are typically used to send “bulk” or large quantities of text messages. Aggregators typically inject messages on behalf of other companies and charge their clients for the service. Finally, most providers have established relationships between each other to allow for messages sent from one network to be delivered in the other. Fig. shows these three high-level strategies. After entering a provider’s network, messages are sent to the Short Messaging Service Centre (SMSC) [2]· SMSCs perform operations similar to e-mail handling servers in the Internet, and store and forward messages to their appropriate destinations. Because messages can be injected into the network from so many external sources, SMSCs typically perform aggressive spam filtering on all incoming messages. All messages passing this filtering are then converted and copied into the necessary SMS message format and encoding and then placed into a queue to be forwarded to their final destination.



2.2 MODULE DESCRIPTION

Text messages arrive in a provider’s network from a wide variety of sources and are processed by the SMSC before being delivered to mobile devices. In this paper there are four modules which describe the overall implementation of the project.

- Location Selection and Characterization.
- Mathematical Characterization of Emergencies.
- Modelling Emergency Events In Real Environments
- Emergency Scenarios
- Simulating emergency events

2.2.1 Location Selection and Characterization

In this module, for the first time users, the users need to configure the application using various options. The users are given options to configure the application in their mobile, such that options such as emergency numbers with two options, with the name which should be displayed in the messages, the location information, time information, pin information etc. Pin information is given to make the application secure. Such that no one can change the configuration files, to help in emergency [4]. There may be chances of someone to change the configuration files, so as to protect in from these attacks, secure **pin methodology is adopted.**

2.2.2 Mathematical Characterization of Emergencies

The first step in characterizing a cellular network during an emergency is determining delivery time. In particular, we are interested in understanding the minimum time required to deliver emergency messages. If this time is less than the goal of 10 minutes set forth in by the current public EAS policies and the WARN Act, then such a system may indeed be possible. However, if this goal cannot be met, current networks cannot be considered as good candidates for EAS message delivery.

2.2.3 Modelling emergency events in real environment

To determine whether there exists a mismatch between the current cellular text messaging infrastructure and third party EAS, it is necessary to observe such systems during an emergency. However, because large-scale physical security incidents are rare, we apply a number of modelling techniques to help characterize such events. Calculations represent an optimistic minimum time for the delivery of all messages.

2.2.4 Simulating emergency events

EAS over SMS traffic may still improve the physical security of its intended recipients even though it cannot be delivered to the entire population within a 10 minute time period. If such information can be sent without interfering with other traffic, it could be argued that it would remain beneficial to at least some portion of the receiving population. To better understand the impact of this security incident response and recovery mechanism on other traffic, we further characterize a number of emergency scenarios.

2.2.5 Emergency Scenarios

Users having received notification of an emergency are unlikely to maintain normal usage patterns. In particular, users are likely to attempt to contact their friends and/or family soon after learning about such conditions. Here we considered emergency scenarios like Accident, heart attack, lost location and struck to thief. Alert message will be sent immediately to the emergency numbers like friends or relatives number, to whoever configured initially in first module.

2.3 FINDING A DEVICE

Delivering messages in a cellular network is a much greater challenge than in the traditional Internet. Chief in this difficulty is that users in a cellular network tend to be mobile, so it is not possible to assume that users will be located where we last found them. Moreover, the information about a user’s specific location is typically
limited. For instance, if a mobile device is not currently exchanging messages with a base station, the network may only know a client’s location at a very coarse. Accordingly, the SMSC needs to first find the general location for a message’s intended client before anything else can be done [5].

A server known as the Home Location Register (HLR) assists in this task. This database acts as the permanent repository for a user’s account. When a request to locate a user is received, the HLR determines whether or not that device is currently turned on. If a mobile device is currently powered off, the HLR instructs the SMSC to store the text message and attempt to deliver it at another time. Otherwise, the HLR tells the SMSC the address of the Mobile Switching Centre (MSC) currently serving the desired device. Having received this location information, the SMSC then forwards the text message on to the appropriate MSC.

3 MODELLING EMERGENCY EVENTS IN REAL ENVIRONMENTS

To determine whether there exists a mismatch between the current cellular text messaging infrastructure and third-party EAS, it is necessary to observe such systems during an emergency. The input and output design is concentrated carefully.

3.1 INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

3.2 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should identify the specific output that is needed to meet the requirements, Select methods for presenting information and Create document, report, or other formats that contain information produced by the system.

3.3 MATHEMATICAL CHARACTERIZATION OF EMERGENCIES

The first step in characterizing a cellular network during an emergency is determining delivery time. In particular, we are interested in understanding the minimum time required to deliver emergency messages.

$$T = \frac{15{,}000\ msgs}{1\ campus}\ x\ \frac{1\ campus}{8\ sectors}\ x\ \frac{1\ sector}{8\ SDCCHs}\ x$$

$$1\ SDCCH$$

$$\sim 0.25\ \frac{msgs}{sec}$$

$$\sim 37.52\ sec$$

Stand-alone Dedicated Control Channel (SDCCH) is used in the GSM system to provide a reliable connection for signalling and Short Message Service (SMS) messages [3]. Given that most sectors have a total of eight SDCCHs that it takes approximately 4 seconds to deliver a text message in a GSM network. Tech would require the following amount of time to deliver single message to 15,000 recipients. Because the contents of emergency messages are likely to exceed the 160 character limit of a single text message, providers and emergency management officials have estimated the number of messages is likely to increase by at least four times

$$T = \frac{15{,}000\ msgs}{1\ campus}\ x\ \frac{1\ campus}{8\ sectors}\ x\ \frac{1\ sector}{8\ SDCCHs}\ x$$

$$1\ SDCCH\ x\ 4\ msgs$$

$$\sim 0.25\ \frac{msgs}{sec}$$

$$\sim 3752\ sec$$

$$=62.5\ mins$$

The above calculations represent an optimistic minimum time for the delivery of all messages.

3.4 EFFICIENT SOLUTIONS USING

CURRENT EAS

The experiments in the previous section demonstrate the inability of current cellular infrastructure to support emergency-scale messaging. Significant changes to the network could potentially make such systems more useful. The most promising of such solutions is cell broadcast. Instead of the point to point delivery of messages in current networks, cell broadcast would allow for the rapid dissemination of emergency information through point to multipoint communications.

Such a system could reach the majority of cellular users in an area without requiring knowledge of each particular user's location. This option is backed by the Commercial Mobile Service Alert Advisory Committee, which is currently working on developing standards documents. However, the timeline for the deployment of this standard is not currently known. In the absence of this change, currently deployed third-party
EAS could be effectively used to contact limited subsets of people in an affected area. On a University campus, for instance, sending emergency alerts to faculty members first would allow for a message to manually be amplified.

The minimum time to distribute a single emergency message to the faculty is

$$T = \frac{600\ msgs}{1\ campus}\ x\ \frac{1\ campus}{8\ sectors}\ x\ \frac{1\ sector}{8\ SDCCHs}\ x\ 1\ SDCCH$$

$$\sim 0.25\ msgs/sec$$

=37.5 sec

Similarly, the time to send a long message requiring the delivery of four messages would require the following minimum delivery time.

$$T \quad = \frac{600\ msgs}{1\ campus}\ x\ \frac{1\ campus}{8\ sectors}\ x\ \frac{1\ sector}{8\ SDCCHs}\ x$$

$$1\ SDCCH\ \ x\ 4\ msgs$$

$$\sim 150\ sec$$

=2.5 *mins*

Given that these minimum times are more than an order of magnitude smaller than those associated with directly messaging every person on campus.

4 CONCLUSION

Cellular networks are increasingly becoming the primary means of communication during emergencies. Riding the widely held perception that text messaging is a reliable method of rapidly distributing messages, a large number of colleges, universities, and municipalities have spent tens of millions of dollars to deploy third-party EAS over cellular systems.

However, this security incident response and recovery mechanism simply does not work as advertised [6]. Through modelling, a series of experiments and corroborating evidence from real-world tests, we have shown that these networks cannot meet the 10 minute alert goal. Moreover, we have demonstrated that the extra text messaging traffic generated by third-party EAS will cause congestion in the network and may potentially block upward of 80 percent of normal requests, potentially including calls between emergency responders or the public to 9-1-1 services. Accordingly, it is critical that legislators, technologists, and the general public understand the fundamental limitations of this mechanism to safeguard physical security and public safety and that future solution are thoroughly evaluated before they are deployed.

5 REFERENCES

[1] "Earthquake and Tsunami Warning System (ETWS); Requirements and Solutions," Technical Report 3GPP TS 23.828 v2.0.0., 3rd Generation Partnership Project, 2008.

[2] "Technical Realization of Short Message Service Cell Broadcast (SMSCB)," Technical Report 3GPP TS 03.41 v7.5.0., 3rd Generation Partnership Project, 2000.

[3] "Technical Realization of the Short Message Service (SMS)," Technical Report 3GPP TS 03.40 v7.5.0., 3rd Generation Partnership Project, 2002.

[4] Agence France-Presse, "Hoax Text Message Spreads Tsunami Terror in Indonesia," http://www.breitbart.com/article.php?id=070606101917.31jf2eyb&show_arti, 2007.

[5] D. Andersen, "Mayday: Distributed Filtering for Internet Services," Proc. USENIX Symp. Internet Technologies and Systems (USITS), 2003.

[6] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing Internet Denial of Service with Capabilities," Proc. ACM Workshop Hot Topics in Networking (HotNets), 2003.