**Protect Yourself Android App**

**ABSTRACT:**

Cellular text messaging services are increasingly being relied upon to disseminate critical information during emergencies. Accordingly, a wide range of organizations including colleges and universities now partner with third-party providers that promise to improve physical security by rapidly delivering such messages. Unfortunately, these products do not work as advertised due to limitations of cellular infrastructure and therefore provide a false sense of security to their users. In this paper, we perform the first extensive investigation and characterization of the limitations of an Emergency Alert System (EAS) using text messages as a security incident response mechanism. We show emergency alert systems built on text messaging not only can meet the 10 minute delivery requirement mandated by the WARN Act, but also potentially cause other voice and SMS traffic to be blocked at rates upward of 80 percent. We then show that our results are representative of reality by comparing them to a number of documented but not previously understood failures. Finally, we analyze a targeted messaging mechanism as a means of efficiently using currently deployed infrastructure and third-party EAS. In so doing, we demonstrate that this increasingly deployed security infrastructure does not achieve its stated requirements for large populations.

**EXISTING SYSTEM:**

Accordingly, SMS messaging is now viewed by many as a reliable method of communication when all other means appear unavailable. In response to this perception, a number of companies offer SMS-based emergency messaging services. Touted as able to deliver critical information colleges, universities, and even municipalities hoping to coordinate and protect the physical security of the general public have spent tens of millions of dollars to install such systems. Unfortunately, these products will not work as advertised and provide a false sense of security to their users.

**DISADVANTAGES OF EXISTING SYSTEM:**

Accordingly, a wide range of organizations including colleges and universities now partner with third-party providers that promise to improve physical security by rapidly delivering such messages. Unfortunately, these products do not work as advertised due to limitations of cellular infrastructure and therefore provide a false sense of security to their users.

**PROPOSED SYSTEM:**

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 webpages, 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. After entering a provider’s network, messages are sent to the Short Messaging Service Center (SMSC). 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.

**Emergency event characterization:** Through modeling 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.

**Measure EAS over SMS for multiple emergency scenarios:** We provide data to debunk the common assertion made by many third-party vendors that large quantities 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 realworld example that very closely mirrors the results of our simulations.

**Quantify collateral damage**: We characterize the presence of the additional traffic generated by thirdparty EAS over SMS and show that such traffic causes increased blocking of normal calls and text message, potentially preventing those in need of help from receiving it. We also discuss a number of ways in which these networks can cause unexpected failures (e.g., message delay, message reordering, alert spoofing).

**ADVANTAGES OF PROPOSED SYSTEM:**

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.

In the past few years, a significant number of third-parties offering to deliver alert messages (and other information services) via text messaging have appeared. Citing the need for improved delivery targeted to a highly mobile population, many such services advertise text messaging as an instant, targeted disseminator capable of delivering of critical information to tens of thousands of mobile phones when it is most needed. These systems have been extensively deployed on college and university campuses throughout the United States.

**MODULES:**

* Location Selection and Characterization
* Mathematical Characterization of Emergencies
* MODELING EMERGENCY EVENTS IN REAL ENVIRONMENTS
* Emergency Scenarios

**MODULE DESCRIPTION:**

**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. There may be chances of someone to change the configuration files, so as to protect in from these attacks, secure pin methodology is adopted.

**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.

**MODELING 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. However, because large-scale physical security incidents are rare, we apply a number of modeling techniques to help characterize such events. Calculations represent an optimistic minimum time for the delivery of all messages.

**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.

**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 whom ever configured initially in first module.

**SYSTEM REQUIREMENT**

**HARDWARE REQUIREMENT**

* CPU type :    Intel Pentium 4
* Clock speed                 :    3.0 GHz
* Ram size                      :    512 MB
* Hard disk capacity       :    40 GB
* Monitor type                :    15 Inch color monitor
* Keyboard type             :     internet keyboard
* Mobile : ANDROID

**SOFTWARE REQUIREMENT**

* Operating System :  Android
* Language          :  ANDROID SDK 2.3
* Back End                    :    SQLite
* Documentation   :    Ms-Office