Proactive Detection and Recovery of Lost Mobile Phones

Chen Hui Ong[1], Nelly Kasim[1], Sajindra Jayasena[1], Larry Rudolph[2], Tat Jen Cham[3]
[1]National University of Singapore, [2]CSAIL, MIT, [3]Nanyang Technological University

***Abstract* – This paper describes the successful implementation of a prototype software application that independently and proactively detects whether a mobile phone is lost or misused. When the mobile phone is detected as being lost or misused, the application takes steps to mitigate the impact of loss and to gather evidence. The goal is to aid in the recovery of the mobile phone. The prototype works regardless of the cellular infrastructure the mobile phone is operating in and makes minimum demands on the owner of the mobile phone. The prototype was developed on Nokia 6600 mobile phones that run Symbian Operating System 7.0s. Development was done using Nokia's Series 60 Developer's Platform 2.0.**

***Index Terms* – Cellular telephone sets, loss detection, tracking.**

I. INTRODUCTION

Many mobile phones are lost every year. According to estimates [1][2][3], 1 million mobile phones were lost in United Kingdom in a 10-months period between November 2002 and September 2003. Australia too reported 100,000 mobile phones lost in 2002. In Singapore, 3000 mobile phones were reported lost to the police in 2003.

Mobile phones may be stolen through criminal acts, such as assault, robberies and pick-pocketing, or lost through the carelessness of the owners. Stealing a mobile phone is becoming an increasingly common motivation for crime and this phenomenon is causing concern from regulators and the police [4][5]. A mobile phone that is lost can be resold for profit or it can be used to make phone calls using the existing connection [6]. Besides the monetary incentives of stealing mobile phones, personal information stored in mobile phones, such as contact lists, calendar, can also be stolen [6]. As the line between mobile phones and personal digital assistant gets blurred, the potential impact of lost information becomes more severe.

A. Motivation

Stealing mobile phones is profitable and the profits have kept theft rates high. Despite the high loss rates, today's solutions for recovering a lost mobile phone and for protecting the information stored in the mobile phone are very inadequate.

Firstly, the detection scheme is inadequate. Even though mobile phones have fairly significant computing powers, today's mobile phones do not independently detect if it is lost. Only when the owner detects and reports the loss does recovery and loss mitigation process start.

Secondly, the loss mitigation process is inadequate and only addresses the issue of minimizing financial loss. When an owner loses a mobile phone, the loss is usually reported to the cellular service provider, who will then disable the phone number associated with the Subscriber Identity Module (SIM) [8]. This action ensures that anyone who picks up the lost mobile phone (for convenience, we shall label such people "thieves") is unable to "freeload" on owner's call time. However, it does not prevent the thief from using the phone with another SIM nor to extract the owner's personal information from the phone.

In addition to phone number disablement, some cellular service providers are also able to perform IMEI blocking. The International Mobile Equipment Identifier (IMEI) is a unique number assigned to every mobile phone. When a mobile phone is turned on, the mobile phone will broadcast its IMEI as it attempts to connect to a base station. Some cellular service providers have upgraded their equipment to listen for these IMEI broadcasts. These service providers can reject any attempt to connect to its base station by IMEI corresponding to stolen mobile phones. IMEI blocking requires that either the owners of lost mobile phones to

remember the IMEI of their mobile phones or that the service provider tracks the IMEI of their subscribers. Unfortunately, not all service providers have the necessary infrastructure to support IMEI blocking. Moreover, to be effective, the lost IMEI needs to be perpetuated across all service providers. Ideally, the owner should receive the same reassurance that the mobile phone is not misused regardless of whether the thief stayed on the same cellular provider or moved to another country.

Phone number disablement is useful in minimizing the financial losses that can be incurred for the owner. IMEI blocking prevents the same phone from being used. However, these responses are only triggered when the owner detects the loss and reports it to the cellular service provider. Moreover, the responses do not address the loss of privacy that occurs when mobile phones are lost. Neither do the methods help the owner track where the mobile phone might be and who is using the mobile phone.

B. Objective

The objective of our work is to design a mobile phone application that independently and proactively checks if the phone is lost. If a loss is detected, the mobile phone shall a) gathers evidence to aid in the recovery of the mobile phone and b) minimize the information lost.

We built a proof-of-concept prototype on a Nokia 6600 mobile phone running Symbian operating system 7.0s [9]. Development was done using Nokia's Series 60 development platform 2.0 using Symbian C++.

C. Organization of paper

The design of the application is described in Section II. This is followed by a detailed description of the modules implemented in the prototype in Section III. The limitations of our current design and future work are described in Sections IV and V respectively. Section VI wraps up with the conclusions.

II. OVERVIEW

A. Design Objectives

1) Versatile detection mechanism: The application should not be so heavily dependent on the owner's vigilance and the thief's actions. We set a requirement for the detection mechanism to be able to detect its loss regardless of whether the owner reported the loss and whether the thief changed the SIM.

If the owner reported the loss, the mobile phone needs to be notified as soon as possible of its lost status. The ease of notifications is dependent on whether the thief changed the SIM. Notifying a mobile phone whose SIM did not change is relatively trivial, since the phone number of the mobile phone remains unchanged. However, if the SIM is changed, the task of notification becomes non-trivial. In the event that the owner did not report the loss, the mobile phone will have to independently determine its status. To summarize, we consider four scenarios:

a. when the owner reports the loss and the SIM card remains unchanged;
b. when the owner does not report the loss and the SIM card remains unchanged;
c. when the owner reports the loss and the SIM card is changed;
d. when the owner does not report the loss but the SIM card is changed.

2) Loss mitigation and tracking: Once a mobile phone is detected to be lost, the application should proactively gather evidence on who the thief is and where the mobile phone is. In addition, the application should also attempt to mitigate the loss of owner's privacy.

3) Minimum infrastructure upgrades: Any communications between the mobile phone and the owner should occur regardless of the cellular network that the mobile phone is used in. This means that the communications should rely on commonly used cellular services, such as Short Messaging Service (SMS), Multimedia Messaging Service (MMS) and General Packet Radio Service (GPRS), rather than define a whole new communication system.

4) Minimum demands on the owner: The application should make minimum demands on the owner of the mobile phone. The application should not, for example, assume that owners will remember the IMEI number.

B. Overview of Application

Our design assumes the presence of 3 players:

a. Owner,
b. A trusted third party, and

c. Application.

The trusted third party acts a remote entity that the application communicates with. It acts as an interface between the owner and the application. The third party may be a trusted friend, a mobile phone theft monitoring service or a cellular service provider.

The prototype application followings the high level functionality depicted in Figure 1.

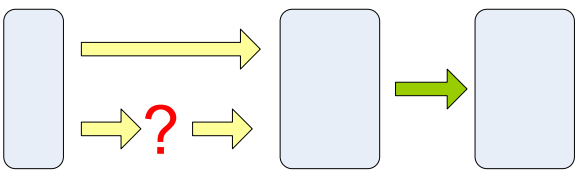

Figure 1 High Level Functionality

In the design of our prototype, we decoupled the flow into distinct segments, each representing one specific responsibility (detection mechanism, loss mitigation and evidence gathering, or evidence gathering). Each box can be viewed as a black box, with designated input/output where new detection mechanism can be added easily within the scope of the first black box, without difficulties.

The detection mechanisms module is responsible for detecting loss. When the detection mechanism unambiguously determines that the mobile phone is indeed lost, the application sets its status to LOST and initiates the loss mitigation and evidence gathering mechanisms. However, in many scenarios, the application is unable to unambiguously determine if the mobile phone is lost. In this event, the application sets its status to SUSPECTED_LOST. The application will send out a request for confirmation from the trusted third party. Only when it receives a reply that confirms the mobile phone is lost will the application confirm that the mobile phone is lost.

Once the detection mechanisms confirm that the phone is lost, the mobile phone will begin loss mitigation and evidence gathering. Loss mitigation refers to a set of activities that is aimed at reducing the possibility of fraud, identity theft and loss of privacy.

The objective of performing evidence gathering is to provide sufficient evidence of who is using the phone and where the phone is. The evidence collected is submitted to the trusted third party.

III. Detailed Description

A. Architecture

The architecture of our prototype application is shown in Figure 2. Our prototype was built by interfacing with six Symbian services: Etel (telephony) server, camera server, SMS message type module (MTM)), MMS MTM, voice system and the call log engine.

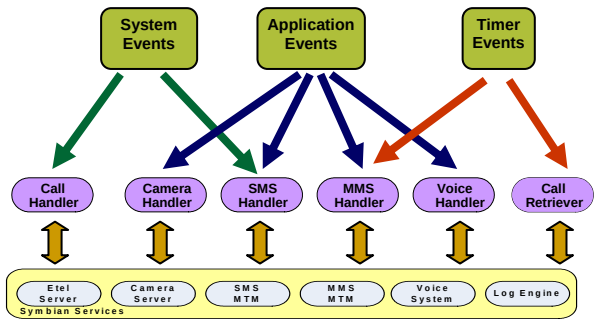

Figure 2 Architecture

As the Symbian operating system is a real-time operating system, most calls are made asynchronously. Besides the SMS Handler and MMS Handler, all other modules use asynchronous access to interface with Symbian's services. The call handler and call retriever uses Symbian's active objects to access the telephony server and call log engine. The camera server, voice system, and log engine are accessed through observer-based asynchronous access.

There are four types of triggers for our application. The first trigger is a startup-event trigger. When the mobile phone starts up, our application is loaded as a background process. A timer is started and all handlers are initialized. The MNC / MCC change and call pattern detection mechanisms is initiated. The second type of trigger is a signal from an incoming SMS. The signal triggers the application's SMS notification detection mechanism. The third type of trigger is also a signal trigger, this time from an incoming call. When an incoming call arrives and the thief answers the phone call, the voice and camera handlers, which are asynchronous observers, begin to collect voice samples and

Confirmed status

Detection Mechanisms

suspicion

Confirmation

Loss mitigation + Evidence Gathering

take pictures of surroundings. The fourth trigger type is by time. At 24-hours intervals, the active scheduler will send the application an event. If the phone's status is not LOST, the call pattern detection mechanism starts. If the phone's status is LOST, the periodic evidence collection mechanisms are started.

B. Detection Mechanism

In the prototype, we defined three different detection mechanisms:

a. SMS notification.
b. Call pattern.
c. MNC / MCC change detection.

The different detection mechanisms are used in different scenarios to detect loss. Table 1 summarizes the scenarios where the detection mechanisms are useful.

	SIM unchanged	**SIM changed**
Owner reports loss	SMS, Call pattern	MNC/MCC change, call pattern
Owner does not report	Call pattern	MNC/MCC change, call pattern

Table 1 Detection Mechanisms used for each Scenario

1) SMS notification. Short Messaging System (SMS) are a common service provided on almost all cellular phones. If the owner reports the loss to a trusted third party, the third party will first attempt to notify the mobile phone through SMS notification. If the SIM of the mobile phone has not been changed, the SMS handler will intercept every incoming SMS message, check if the message is a notification and unobtrusively delete all notification messages. Next, the application will set its status to LOST.

2) MNC / MCC change detection. The combination of MNC (Mobile Network Code) and MCC (Mobile Country Code) is a unique identifier for every cellular network operators. MNC / MCC codes are broadcasted by cellular service provider and stored in the mobile phone. A change of MNC / MCC indicates that the mobile phone operating under a different cellular operator, which may be caused by a change of SIM. At startup and 24-hourly intervals, the call handler will check the MNC / MCC. If the MNC / MCC identifier is changed, the application sets its status to SUSPECTED_LOST and attempts to perform status verification.

3) Call Pattern. Each mobile phone user has a unique signature in their call pattern. The signature may include the type of numbers called, how long the calls usually are and when they are made. In our prototype, we check the call logs every 24 hours. We apply the heuristic that at least 3 of the outgoing numbers should remain the same over every 24 hour period. If the heuristic is not followed, the application sets its status to SUSPECTED_LOST and begins status verification.

C. Status Verification

The flow chart in Figure 3 illustrates the process that the application follows to verify its status with the trusted third party.

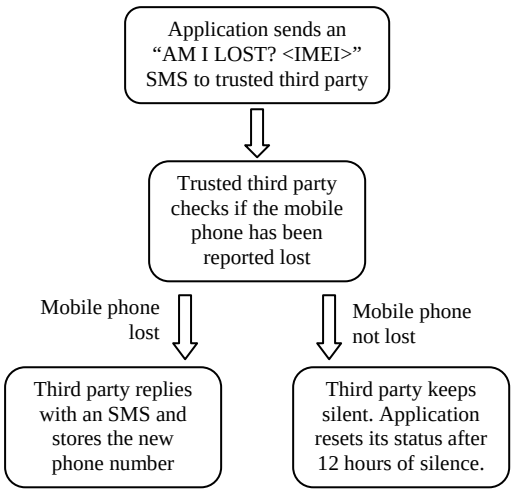

Figure 3 Events flow for Status Verification

The application sends the IMEI of the mobile phone to identify the phone. When the trusted third party receives the SMS, it checks if the loss has been reported. If it has, the trusted third party immediately replies to the application that the mobile phone is lost through SMS. The SMS handler will intercept this verification SMS in the way described in SMS notification detection mechanism. Otherwise, the trusted third party will contact the owner and the contacts provided by the owner. By contacting the owner or the owner's friends, the trusted third party proactively prompts the owner to check on the mobile phone. Depending on the response from the owner, the third party will choose the appropriate response to the application.

D. Loss Mitigation

Once the status of the phone is determined to be LOST, the call log handler will delete the

personal contact information stored in the mobile phone. This was implemented to prevent a misuse of owner's personal contact information by the thief or unauthorized owner.

E. Evidence Gathering

During evidence gathering, the application collects evidence to determine the whereabouts of the mobile phone and the person using the mobile phone. The evidence the application gathers are:

1) IMEI. For tracking to be effective, the lost mobile phone needs to be uniquely identified. Since the SIM of a mobile phone can be changed easily, the phone number of a lost mobile phone is a poor identifier of the mobile phone. In our prototype, we use the IMEI to identify each lost mobile phone. At start up and at 24 hour intervals, the call handler will poll for IMEI information. The information is submitted together with cellular network information to the trusted third party.

2) Cellular network information. To keep track of where the mobile phone is, we collect cellular network information. In particular, the call handler tracks the MNC and MCC to identify which cellular service provider is currently providing service to the mobile phone. The call handler also extracts the cell identifier to pinpoint the base station that the mobile phone is connected to. However, collecting this information only provides a geographical area where the mobile phone might be operating. Further evidence is needed to identify where the mobile phone is and the thief using the phone.

3) Call Records. The call retriever module also collects the call log of the mobile. The call log contains the list of telephone numbers that the thief is in contact with and will also describe the thief's unique call pattern. The unique call pattern can be used to identify the thief. Call records are retrieved every 24 hours and submitted as evidence.

4) Image capture. The Nokia 6600 has a built in camera. Incoming call signals trigger the camera handler to power up the camera and take a picture. When the call ends, the picture is submitted as evidence.

5) Voice recording. The aim of voice recording is to collect conversation samples of the thief. In our implementation, voice recording is triggered when there are incoming call signals. Short snippets of the conversation are stored in WAV format. Recording stops when the size of the WAV file exceeds a predetermined threshold. The file is submitted as evidence when the call ends.

F. Evidence Submission

In our prototype implementation, Multimedia Messaging Service (MMS) is used by the application to submit evidence to the trusted third party. The evidence submission engine will group IMEI and cellular network information together into a single MMS. Call records, images, voice recordings are sent out as separate MMS as and when they are ready for submission.

One of the fringe benefits of using MMS is that the trusted third party can extract the most current phone number used by the thief if the number is sent over the network. This will ensure that the trusted third party can keep in contact with the application.

IV. LIMITATIONS

A. Inability to access SIM libraries

The design and implementation of the prototype was limited by the public APIs available on Symbian 7.0s developer's kit. One of the most challenging tasks was to work around the inability to access the SIM and any information stored in the SIM. Accessing the SIM requires special developer's privileges, which were unavailable at the time of the development. Some of the limitations introduced as a result are:

a. The MNC/MCC detection mechanism is designed as a work-around the inability to uniquely identify each SIM. Each SIM has a unique International Mobile Subscriber Identifier (IMSI) which can be polled to determine if the SIM has changed. As the interface to access the SIM is unavailable, the prototype uses MNC / MCC as the detection mechanism. The mechanism suffers from false negatives when thieves substitute SIMs from the same cellular network operator as the original SIM. In addition, the detection mechanism suffers from unnecessary false positives when a mobile phone is auto-roaming.

b. When gathering evidence, we will ideally like to find out the IMSI of any new SIM used by the mobile phone. However, this information cannot be extracted.

B. GPRS as a form of communications

The communications between the trusted third party and the lost mobile phone can be made more robust by using different communication technologies. One obvious choice is the use of General Packet Radio Service (GPRS). GPRS is an obvious choice for communications because the mechanism is cost-effective and reliable. GPRS can be used to:

a. Regularly poll a designated web server for the status of the mobile phone.

b. Upload evidence gathered by the mobile phone to a designated portal. The portal allows the owner or law-enforcement officials real time access to the evidence collected.

In order to avoid invoking the thief's suspicions, the communications between the application and the trusted third party needs to be set to silent mode. However the implementation of GPRS evidence submission works only with pop-ups to select the GPRS channel and trusting the digital certificate of the destination secure https connection. There was insufficient documentation on the HTTPS API for Symbian and HTTPS support for GPRS connection to a secure server. Due to these reasons, the GPRS functionality was not implemented fully in this prototype.

V. FUTURE WORK

One of our immediate goals is to allow the application to run stealthily in the background and to make it more challenging for the thief to delete our application. Currently, our application runs as a regular Symbian process and can be observed using third party software such as AppMan [12]. A thief can easily stop our application from running. This track of work will ensure that the thief remains unaware that our application is running.

The other track of future work is to use machine learning for call pattern recognition. In our prototype, we used a simple heuristic to perform call pattern recognition. The heuristic is not robust against a savvy thief. Machine learning can help in designing a more robust call pattern recognition mechanism. For example, it what features are important in distinguishing one user's call pattern from another user's is not well understood, and neither is there a quantitative measure that can be used to measure the difference between call patterns. Machine learning techniques can give us answers to those questions.

VI. CONCLUSIONS

This paper describes the features and methods used to implement an application that proactively and independently discovers if a mobile phone is lost through SMS notification, MNC / MCC changes and call pattern changes. Should the detection mechanisms indicate that the mobile phone is lost, the application will delete the phone book to mitigate potential information theft and gathers evidence of the location of the mobile phone, the call records of the thief, images of the surroundings and audio snippets of the thief's conversations. The evidence is submitted through MMS to a trusted third party, who can track the location of the mobile phone.

VII. ACKNOWLEDGEMENTS

This prototype was built as a class project in SMA5508: Pervasive Computing in Spring 2004. The equipment was provided by the class.

VIII. REFERENCES

[1] Australian Mobile Telecommunication Association. The Mobile Phone Industry's Lost and Stolen Program. http://www.amta.org.au/default.asp?Page=258&Format=print_3. 15 September 2003.

[2] ChannelMinds. One Million Mobiles Missing. http://www.channelminds.com/article.php3?id_article=991. 1 September 2003.

[3] Singapore Police Force. Crime Situation for Year 2003. http://www.spf.gov.sg/statistics/crimesituation/stats2003_handphonetheft.htm.

[4] Time Europe. A Call for Help. Available: http://www.time.com/time/europe/magazine/article/0,13005,901020311-214207,00.html. 4 March 2002.

[5] Office of Senator Manny Villar. CellFone Theft Getting out of Control. http://www.senate.gov.ph/press_rel/villar1_sept30.htm. 30 September 2004.

[6] The Chase Law Group. Cellular Phone Fraud. http://www.thebestdefense.com/Crimes/white_collar/cellular_phone_fraud.html.

[7] Yahoo India News. Thieves make off with Mossad Chief's Phone. http://in.news.yahoo.com/040311/137/2bxsj.html. 11 March 2004.

[8] GSM World. Industry Takes Lead to Halt Mobile Phone Theft.

http://www.gsmworld.com/news/press_2004/press04_13.shtml. February 2004.
[9] Forum Nokia. Nokia 6600 Device Specifications. http://www.forum.nokia.com/main/0,,016-2067,00.html?model=6600.
[10] Forum Nokia. http://www.forum.nokia.com/main.html.
[11] FAQ: How to Flash / Repair / Unlock Nokia Mobile Phones. http://gsmsearch.com/faq/nokiaflasher.html. 3 October 2003.
[12] SymbianWare: AppMan. http://www.symbianware.com/product.php?id=appman60&pl=n3650.