Architecture for Lost Mobile Tracker Application

Jude Joseph Lamug Martinez and Nelson Widjaya

Abstract—**The aim of this paper is to analyze existing mobile application's architecture and design a new one based on it, in addition, it seeks to implement the application prototype as a proof of concept of the designed architecture. The main benefit of this research is to provide a base architecture for java mobile developers in order to develop a tracking application for lost mobile phones. The observations gathered on existing mobile applications show that most of the mobile applications in tracking lost phones are focused on three characteristics, which are client to server communication, SIM card data retrieval, and mobile application activation event. The result of this research is the application prototype that tracks lost mobile phones. The application prototype implements the architecture analyzed from the characteristics of existing mobile applications which are used to track lost mobile phones.**

Index Terms—**Architecture, Mobile Phone Application, Prototype, Security, Tracker.**

I. Introduction

Since its first founded and used by the public in 1973, the usage of mobile phones have grown so massively. It is not a luxurious item anymore; it is now our part of lifestyle. In the United States, there are over 223 million mobile phone users over the age of 13 in 2010 [1]. Following the studies, these users have used their mobile phone not only for voice call, but also for various activities. Such activity includes accessing the web via their mobile phone, streams like audio and video, downloading applications, and much more. Indonesia ranked 6th position of the countries which have the largest number of mobile phone users in 2010 with an estimate of 116 million users (with China as the 1st position, having 585 millions of mobile phone users) [2]. In the future, these numbers might be increased, due to the development of technologies.

The types of the mobile phones are also various depending on the technology that it possesses. Smart phones are one of many famous mobile phone types on the market now. Statistics show that 48% usage of smart phones can aid a businessman [3] due to so much technology that it possess. In the United States, based on Nielsen report on 2010, 31% of United States citizens have a smart phone as their mobile phone. Not only that, the eMarketer predicts that smart phone owners might increase to 43% of the United States mobile population by 2015 [4].

These types of mobile phones, due to the technology it possess, are not cheap. Their prices range from $100 to over $900. Knowing that the number of users are so massive on the past years, how it affects our lifestyle, and how it is so expensive, security has become an issue that we have to think about.

Since mobile phones are our part of lifestyle, somehow, we would like to store data, or any other information which is private to our mobile phones. The survey conducted on United States by security firm AVG on 2010 shown that 84% of mobile phone users use the same mobile phone for both professional and personal tasks, 66% respondents saying that they kept personal data such as email address, name, contact lists, photos, videos, anniversary and personal dates on their mobile phones. And 23% of respondents keep sensitive data such as passwords on their mobile phones [5]. Consider if the mobile phones which contain those data are lost or stolen. What if any other people have gained possession of the mobile phones and see those data? It will lead into another crime! And knowing these facts, even though mobile phones have been so near to us, sometime mobile phone users tend to be too "lazy" to secure their own mobile phones. The same survey also shows that less than half respondent of the survey used phone locks or any other security measures to handle mobile phone theft.

The number of mobile phone theft case is around 1.3 Million every year according to extensive research by Continental Research [6]. On the same research, many mobile phone theft cases happened because the thief comes after the selling value of the mobile phone itself, which target mostly smart phones. Therefore, a security measure needs to be undertaken in order to reduce or avoid the mobile phone theft cases.

The need for security has been a demand due to the problems stated above. Since most of the targeted mobile phone thefts are mainly smart phones, which support mobile applications, therefore, a security measure from the application can be implemented to reduce the number of mobile phones theft. Such mobile application might include tracking the mobile phones activity such as unauthorized SIM card change, or blocking the usage of mobile phones itself, or also tracking where the mobile device's location is.

However, many mobile applications have been developed under these ideas. Some of those mobile applications have some advantage and disadvantage between one another, and have developed under various platforms. Therefore, the goal of this research is to implement a prototype of lost tracker mobile application based on analysis of current existing mobile application to track any unauthorized SIM card change or any behavior that can be assumed the mobile phone is lost, also to implement the lost tracker mobile service to distribute any data regarding the stored mobile data, and report if the stored mobile data is lost, under java platform.

Manuscript received May 7, 2012; revised June 5, 2012.

Jude Joseph Lamug Martinez is with Philex Mining Corporation in Pasig City, Manila, Philippines.

Nelson Widjaya is with Voyage Indonesia Technology.

II. Problem Analysis

A. Analysis of Existing Studies

Analysis on current studies means any techniques or studies that have been conducted by a person or a company.

GSM Europe, one of the companies that represent the interests of mobile operators worldwide, has studied about possibilities in securing a mobile phone from theft. They said, in order to secure a mobile phone from a mobile theft, there are three families to secure a mobile phone:

1) Network *Family*, which is concerned more to the client and server architecture.
2) *Mobile* User *Family*, which is concerned more to the authentication of the real user by prompting a password.
3) Smart *Card Family*, which is concerned more to the SIM card.

Another study made by Vincent Chern, which proves that one of the methods to track a lost mobile phone is by the client-server architecture. The communication between the two can be established by HTTP connection or via Short Messaging Service [7].

Another study by Victoria Harrington and Pat Mayhem also found that the behavior of mobile phone theft mainly is concerned on the SIM card, which means they might change the SIM card to a new one so the real user does cannot call his mobile phone [8].

B. Analysis on Device Oriented Architecture

Analysis on device oriented structure means any technique or architecture to overcome a lost mobile device that has no connection with software. It is focused more on the implementation of the hardware.

Analysis on device oriented structure is considered as important for the authors because they believe that by learning the current available technique or architecture; it can help them to consider about the hardware instead of only focusing on software.

IMEI blacklist is the technique which is mostly used in order to reduce the number of the stolen mobile phone case. Using IMEI, a phone is able to be locked from the provider service, making the phone useless for a thief. This technique is considered as the reason why IMEI for a mobile device exists [9]. By using this technique, it is expected that the number of stolen mobile device case is reduced because it “implants” an idea that stealing a mobile device is no longer a good business proposition [10]. However, it is not as sweet as it sounds, because today’s criminal has found a way to overcome this blacklisting technique. One way is to change the IMEI of a mobile device. Based on BT Cellnet spokesman quoted by BBC [11], the technique of blocking a service via IMEI blacklisting is only temporal. It does not solve the problem of stolen mobile device. A device can be usable again by changing the service provider and changing the IMEI of a mobile device. He said, “*New IMEIs can be programmed into stolen handsets and 10% of IMEIs are not unique*”. By using some tools, a mobile device’s IMEI can be changed, making an IMEI blacklisting useless. However, by law, this action is considered as illegal, and can pay a “high” amount of price if a person is red-handedly found doing such activity. Active on the 4th October 2002, Home Secretary David Blunkett introduced a new law making re-programming IMEI numbers punishable up to five years in jail [10].

Another way to overcome IMEI blacklisting is by taking the blacklisted device to another country. The blacklist database, (or CEIR) sometimes is only usable in certain country. Therefore, in order for a device which is blacklisted in some country to work again, just simply bring them to another country. It is found that some large number of UK blacklisted device find themselves in Italy, Spain and France. The solution for such problems is to make an international blacklist database. Therefore, if a device is already blacklisted in some country, bringing them into a different country won’t save it from being blacklisted. This idea sounds good, but however again, there are some countries that decline such idea due to budget problems, since upgrading their service to support such systems are expensive [10].

Some uninformed thief who does not know about IMEI re-programming or does not have budget to take the device to another country, another option that they have is to sell parts of the mobile device itself. By doing so, they can also make some money out of selling the keypad, monitor, mobile device’s skin or accessories. This is considered as a desperate way since they cannot use or sell the mobile device as a whole.

Finally, even though this technique can be one of many ways to overcome a lost mobile device, it still has many weaknesses. Furthermore, this technique focuses on making the device to be useless after theft, making it a “passive” technique to track a lost mobile phone. Therefore, we cannot solely depend on this technique for overcome a lost mobile device case. The advantage of using this technique is,

The mobile device being blacklisted by the service provider is unable to operate at all even though SIM card is changed.

While the disadvantage of using this technique is, once the mobile device being compromised is blacklisted, it is hard for a device to be un-blacklisted from the black list database.

Focused on “implanting” idea that stealing mobile device is useless, rather than focusing on how to track back the mobile device itself, in most cases, the real user tends to forget to write the IMEI of the mobile phone or simply lose them.

C. Analysis of Existing Mobile Applications

Analysis on existing mobile applications is conducted because this research will focus on making a mobile J2ME application, which means, analyzing existing application might help the authors to create a better application by learning from each advantage and disadvantage. The selection of existing mobile applications was chosen based on platforms. The analyzed platform was conducted in Android, iOS, and Black Berry. The authors have omitted any other platform because the behavior of the mobile application is the same for any other platforms. The authors also analyzed the following mobile applications by reviewing the feedback from various sources and by using the applications.

Based on the analysis of existing studies and existing mobile applications, the authors found these major characteristics:

1) Client–server communication

Most of the analyzed mobile applications have enabled the feature of remote controlling via client and server communication. This is very important because tracking a lost mobile phone needs another media to track the state of the mobile itself. The state of the mobile phone may include the SIM card that it is using currently, the location of the mobile phone, even giving command remotely such as locking the phone.

2) SIM card *change detection*

Most of the application enabled detection of SIM card change. The reason is because this is the general behavior of the thief when he wants to steal a mobile phone. The thief changes the SIM card so it can be re-used.

3) The activation event of the application

Many of the applications have different kinds of methods to activate their application. Some of them activate their application when the phone boots, while others are activated when a request from the server is sent.

III. Solution Design

A. General Design and Architecture

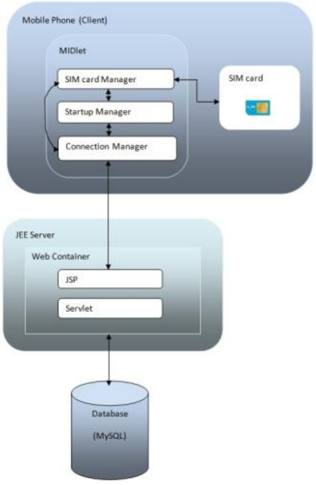

Fig. 1. Design and architecture of application prototype

The figure above shows the global architecture of the prototype based on the analysis. The architecture consists of two important components, which are, the mobile application and the server. In order to develop the mobile application, the authors used J2ME technology. The mobile application component itself consists of the SIM card manager component, the connection manager component, and the startup manager component. For the server component, the authors used J2EE server which consists of JSP and Servlet technologies. The server also communicates with the MySQL database server to store data.

The mobile application component, which is the biggest part of the whole application, has the main purpose to maintain the flow of the application logic, such as how it communicates with AMS (Application Management Service) to manage startup activity of the MIDlet, also manage the retrieval data from SIM card and sends or receives data from server.

The SIM card manager component of the mobile application component does a simple job to manage the current ID of the SIM card embedded on the mobile devices. It first reads the current ID of the SIM card when the mobile device boots up, or when the server requests. Then the component will notify the application (MIDlet) whether the current ID of the SIM card matches the previous SIM card, or matches to the user's predefined SIM card ID. The c client-server manager component maintains a communication from the mobile device with the server. The server (which will be using Servlet and JSP), receives information from the mobile device via SMS (Short Messaging Services), and process the information. After the server process the information, the server will response back to the mobile device via SMS. The reason why the client-server uses SMS as its communication protocol is because SMS does not require any specific configuration to use it. The Server, which is the web container, is using Servlet and JSP technology. They communicate directly to the mobile application via SMS. Any incoming data from mobile application will be stored on database.

B. Solution Technology

The authors used J2ME technology to create the mobile application prototype in the client side (mobile phone), and J2EE technology to create the web application in server side. Each side has their own components and technologies as follows:

1) Technology for connection manager in MIDlet

The main responsibility of this component is to maintain communication between a mobile phone with a server. And to achieve this, SMS is used as a media of communication between the two sides. Figure below describe briefly about the general architecture on how SMS is being sent and received by mobile devices and the server.

2) Technology for startup manager in MIDlet

This component focuses more on starting a MIDlet without user prompts. To achieve this, the MIDlet needs to register connection for the push registry. It can be set statically or dynamically. In this research, the authors used static push registry. Modifying the JAD file, we added MIDlet-Push-1: sms://:50000,MyMidlet,*; This means MyMIDlet will automatically start if any short messages are received from port 50000. For activation when phone boots, the authors used autorun ://:< name of the MIDlet>.

3) Technology for web container in server side

The technology used for the web container is using JSP and Servlet technology. However, in order for a mobile application to communicate with a web application using SMS, SMS gateway is used. Throughout the research, the authors used a "trial version" of commercial software called NowSMS. By using this software, it can retrieve any incoming/outbound short messages and relay them into a web application.

The SMS gateway has responsibility to receive and send short messages to and from a mobile phone, and relay the message to and from the web application as well.

In order to send and receive SMS, the SMS gateway has to support two way messaging. It means that the SMS gateway is not only able to receive, but also send short messages. This is necessary for the server to be able to respond and receive any requests from the mobile phone.

In addition, the authors used GSM modem as the SMSC type of connection. Therefore, a GSM modem capable of doing SMS is also needed.

Below is the detailed design and description for sending and receiving SMS using SMS gateway.

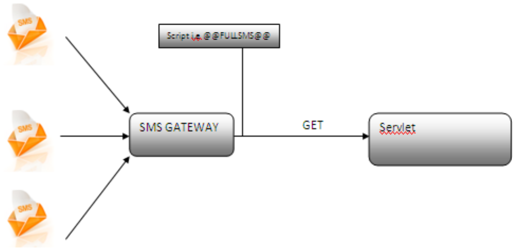

Fig. 2. Receiving an SMS from the server

In order for an SMS gateway to relay the short messages from mobile devices, the scripts within the SMS gateway have to be used. Different SMS gateways have different scripts. For SMS, it uses "@@FULLSMS@@" to retrieve any incoming short messages. After the SMS is retrieved using the SMS gateway script, the SMS is sent via GET method of the Http Request and will be received by the Servlet for further processing.

IV. Observation

There are a lot of existing systems architectures that have been developed, however, many of those applications are not developed under Java platform. The authors then decided to develop the application prototype under Java platform, due to the benefits that it has, including cross platform capability. Based on the analysis of existing studies and existing mobile applications, the authors found these observations based on these major characteristics:

A. *Observation* on *Client-Server Component*

Most of the existing applications have been developed under client-server architecture. This means that the mobile application installed on the stolen mobile can be remotely controlled. The method on how a mobile phone can contact the server can be various depending on different kinds of applications. One way is via internet, as implemented on McAfee Wave Secure theft application for android platform. However, the drawback of this system is the internet needs to be configured for different service providers. It will be good if the thief changed the SIM card to the same provider as the user does, but it will be problematic if the thief changed to a different provider. Since the thief might, or might not configure the internet when the phone boots, especially when the thief knows that the phone has been installed with a lost tracking application. Therefore, the authors have chosen to use SMS as a media to communicate between mobile phone and the server. SMS by nature has give easiness for the user to straightly use this service without any configuration. Therefore, the authors believe by using this, the details of the new SIM card (the thief's SIM card), or location can be quickly reported to the server.

B. Observation on Mobile Phone – SIM card Component

Mobile Phone-SIM card architecture focuses more on how a mobile application can retrieve information from a SIM card. Some of the existing applications analyzed by the authors retrieve the phone number, or the SIM card's IMSI. The author would like to improve the application so it does not only read IMSI and phone number, but also reads MCC, MNC, and cell ID of the SIM card, so it can be used for the user to know the location of the mobile phone.

C. *Observation on Mobile Phone Application activation Related Component*

Existing lost tracker applications require the application to be run on background for it to be fully functional, as implemented by Antidroid Theft for android platform. This might be a major drawback if the thief knows that it runs in the background, and might make the thief to stop the application running in the background which leads the application to be useless. To cover the drawback, the authors thought of a way to develop an application where the application will do action(s) at one point of event, where the application will detect that event, immediately do what the application needs to do, and close itself, without it being run on the background in a long time. This action will consist of the time when the application detects current SIM card and do cross checking with predefined SIM card. If it is different, it will send the information, and then close itself. Another action will be when the mobile phone receives messages through a specific port; the application will automatically boot, immediately do what the server ask it to do, reply back and turn itself off.

V. Result

The result of this research is an application prototype of lost tracking software based on J2ME for mobile phones, while the information provider on the server is based on J2EE. The application on the mobile phone side can track any unauthorized SIM card change, and report it to the server for further action. On the server side, the server can send request to the mobile phone to track the state of the mobile phone, also to receive incoming message from the mobile phone about the mobile phone status. One thing need to be considered is that the application does not cover if the thief does not let the mobile phone boot or the thief intend to sell the parts of the mobile phone. Since the application still resides on the software side, not the hardware side. And also, throughout this research, the testing is more focused on the Sony Ericsson as a proof of concept.

VI. Conclusion

Although mobile phone usage becomes extremely popular right now, users suffer from some major drawbacks. These drawbacks include but are not limited to how they keep their mobile phone secure from mobile phone theft. That is why the authors came up with an idea of creating a mobile application that can track a lost mobile phone.

The aim of this research is to create an application prototype that can track a lost mobile phone and discover the architecture behind it. To accomplish this objective, the authors analyzed some of the existing lost tracking mobile applications, and found out that there are two sides of the coin needed to be fulfilled. They are to create an application on the mobile phone and on the server side.

The application prototype for the mobile side is developed using J2ME and have three main components, which are the client and server component, mobile phone and SIM card component, and mobile phone activation component. The client and server component acts as a component to manage the connection between client and server. The mobile phone and SIM card component acts as how the mobile application retrieves the SIM card data, while the mobile phone activation component manages the activation handler for the application. From what is discussed on the previous sections, this application prototype is different from the existing applications available in the market since the application's architecture comes from learning the advantages and disadvantages of existing applications and further developed using J2ME platform having cross platform abilities.

Based on the testing, this application has fulfilled the predefined aim and scope of the research. Although as mentioned before, this application does not cover for the thief who intended to sell parts of the mobile phone, this application prototype has given proof of the architecture for lost tracker mobile application.

Although the application prototype has achieved its main purpose and fulfilled the requirements given, it is still worth for further study and development. More functionality can be added to the application prototype. Those functionalities include support of data backup, improved accuracy for location tracking, and a less expensive communication between client and server. For the compatibility, it is very outstanding if the MIDlet can be signed with a trusted certificate, and also invents a way to cover theft case which aims for selling mobile phone parts.

References

[1] T. Chillton. (March 31, 2011). Cell Phone Usage Statistics 2010, 2010. [Online]. Available: http://signalnews.com/cell-phone-usage-statistics-2010

[2] A. Hidayah. (2010). Statistik Pengguna Handphone di Indonesia. [Online]. Available: http://www.amipulsa.web.id/2010/10/statistik-pengguna-handphone-indonesia.html [Accessed: March 31, 2011]

[3] T. Tribune. (2010). Smart Phone Statistics. [Online]. Available: http://www.shutupandgoogleit.com/component/content/article/3-smartphone-articles/58

[4] Brownlow. Mark, Smartphone statistics and market share, 2010. [Online].Available: http://www.email-marketing-reports.com/wireless-mobile/smartphone-statistics.htm [Accessed: March 31, 2011]

[5] J. O'Deli, Survey shows we're too lazy about mobile phone security,2011.[Online] Available: http://mashable.com/2011/03/25/mobile-phone-security/ [Accessed: March 31, 2011]

[6] *Mobile Phone Theft*, MobilePhone Insurance, 2009. [Online] Available: http://www.mobilephoneinsurance-uk.co.uk/mobileinsurance-theft/

[7] Chern et al., "System and Method For Locating and Tracking Mobile Telephone Devices Via The Internet," White Paper, United States: Patent, 2002.

[8] V. Harrington et al., "Mobile Phone Theft", *White Paper, Home Office Research*, Development and Statistics Diretorate, 2001

[9] B. Amit. (2008). What is international mobile equipment identity, [Online]. Available: http://www.mobilephonestracker.com/imei/

[10] Blacklisted, Blocked or barred handsets, UnlockMe, 2010. [Online]. Available: http://www.unlockme.co.uk/blacklist.html

[11] BBC, Phone Firms defend security record, 2002. [Online]. Available: http://news.bbc.co.uk/2/hi/uk_news/1749215.stm

[12] Purnama, J2ME Mobile Application: A Customizable Mobile Browser With HTML TO WML Conversion for J2ME Mobile Phones.

[13] *Computer Security: A Practical Definition*, The McGraw-Hill Companies 1999. [Online]. Available: http://www.albion.com/security/intro-4.html

[14] *GSME proposals regarding mobile theft and IMEI Security*. The GSM Association,. London, 2003

[15] Hyfeno, How to check imei number on phone, 2009. [Online]. Available: http://hyfeno.com/how-to-check-imei-number-on-phone/

[16] M. Haydn, What If Your Mobile Phone Gets Stolen, 2010. [Online]. Available: http://www.mobilephonesandsafety.co.uk/what-if-your-mobile-phone-gets-stolen.html

[17] *Techprone*, 5Android Apps To Track and Recover Lost Android Mobile Phone, 2011. [Online]. Available: http://www.techprone.com/5-android-apps-to-track-and-recover-lost-andnroid-mobile-phone/

[18] *AndroidMarket*, McAfee Wave Secure, 2011. [Online]. Available: https://market.android.com/details?id=com.wsandroid&feature=search_result

J. J. L. Martinez completed his Masters in Computer Science at De La Salle University, Manila. Having finished a Bachelor's degree in Computer Science, he worked as an IT specialist and programmer for Philex Mining Corporation in Pasig City, Manila, Philippines. After getting ample experience in the field, he moved to the education sector and ever since worked as an academician, he also worked as a part time IT consultant to one of the projects at Cypress Semiconductor Inc. He is adept to programming (C, Objective C, JAVA (J2SE/J2ME/JEE) and IA32 Assembly Language), troubleshooting hardware and tweaking software is an added hobby. In addition, he is also inclined to curriculum development and managing administrative tasks in line within the education sector. On top of these, he is a member of the Regional Quality Assessment Team (RQAT) CAR for Higher Education in the Cordillera Administrative Region, Philippines, the JAVA Education Development Initiative (JEDI) Community, Philippine Society of IT Educators (PSITE) and Association of Computing Machinery (ACM). Education is a continuous learning process, as such, his research interests includes but is not limited to the fields of Software Engineering, Gaming Technology, Human Computer Interaction (HCI), Pervasive and Mobile Computing.

N. Widjaya finished his bachelor degree in Information Technology (Web Systems) at the Royal Melbourne Institute of Technology (RMIT) Australia and Computer Science at Binus International, Binus University (Indonesia). He is currently working as a Lead Programmer for iPhone Application and Game division in Voyage Indonesia Technology, a company branch of Voyage Group which is one of the popular companies in Japan who mainly focuses on technology development and constructing a fun environment while working to maintain their employee's qualities. With a passion for studying and learning new technologies, at the same time, other countries' culture as well, he is doing his best at perceiving his aims; to be a "multi-talented" IT specialist with "multi-country" qualities.