Securing Application in Mobile Computing

Iehab Al Rassan and Mohannad A. Al Sheikh

***Abstract*—Smart phones and PDAs face major security concerns and problems in changing technology landscape [1]. Security in the mobile computing environment is a serious concern that is important to be addressed. The main motivation of this paper is to come up with a mechanism to ensure user's private data is protected and secured in the event of a mobile device being lost or stolen. We will address how to secure the applications and its data that run on mobile handled devices by providing and offering security capabilities to protect these devices. We will propose a new solution and technique for securing applications in mobile devices to resolve some of the security concerns in mobile computing environment. The proposed solution provides efficient way to secure user's private data in case of mobile device being lost or stolen by sending predefined commands via SMS messages to the stolen or lost mobile device to protect the applications and their data using the necessary action (delete the private data and send back the location information of stolen device to the secondary emergency phone number).**

***Index Terms*—Smart phones, mobile, SMS, GPS, android, security.**

I. Introduction

PDAs and smart phones are equipped with applications that being store sensitive data [2] for example, banking transactions, bank account balance, funds transfers, contact details and payment information. All these sensitive information that need to be secured.

Therefore, Smartphone and PDA phone are goals for thieves and creeps. Sensitive data and important information stored inside the phone device can be easily stolen. That implies there must be a mechanism for protecting user private data and important information stored inside the phone device.

There are many constraints and challenges that exist with mobile applications for examples:

1) Different platform for mobile devices (Windows mobile, IPhone, Symbion, Palm) that lead to challenges in designing and developing different version of the same applications.
2) The developers and designers of the mobile application need to know the different technologies and application programming interface for the different mobile platform.
3) Screen sizing.
4) Different resolution for each screen size and orientation (landscape orientation, portrait orientation and so on).
5) The limitation of input devices and the variations of user interactions such as keypad, touch screen and so on.
6) Text input from the mobile user is difficult to manage and maintain. Battery life is quite limited also it needs to be charge regularly.
7) The processing power is limited.
8) Memory and storage is limited.
9) The limitations that exist in the network bandwidth.
10) Unreliability in the network connectivity
11) The bandwidth is costly.

The developers of the mobile application face these constraints and challenges and must try to design and develop a reliable mobile application and try to overcome these constraints [3].

Manuscript received October 9, 2012; revised March 27, 2013.

Iehab Al Rassan and Mohannad A. Al Sheikh are with the Department of Computer Science, King Saud University (e-mail: irassan@ksu.edu.sa).

II. Related Work

FRAMESEC proposed by [4] it is an application framework that offers a general structure with security technique that facilitates end to end security in mobile computing application.

FRAMESEC is a framework that provides mobile computing applications with the following security aspects: confidentiality, integrity, authenticity, non-repudiation.

The solution that provided by [5] was developed in java micro edition (java2me) for end-to-end security in mobile computing environment. It offers authentication and confidentiality in the transmission between an application server and a mobile device. The confidentiality is reached by the A.E.S Rijndael algorithm. The authentication is reached by the key exchange mechanism used in the proposed solution. However, the solution does not offer services with integrity and non-repudiation.

III. Security Issues in Mobile Computing

Mobile devices seem to be a growing essential in the way of communication it is not a luxury yet gives valuable advantages in our business and personal lives

Sensitive and discrete information of data that is stored inside these devices need a mechanism to safe guard and protect this information. For example, an email application consists of all emails of an individual. Contents of emails might be corporate information, password confirmations, and sensitive company content and bank details. There is an extra risk when the mobile device keeps connecting to the network [6].

The following are the Security issues in mobile computing:

1) Authenticating the right user of the device. (Username/Password) challenged on application access. The objective is to prevent the attacker from getting the sensitive data and secret information once a device has been stolen. In addition, it is highly recommended to

encrypt these secrete data.

2) Malicious code. It is necessary to prevent malicious code from executing in the device; this could damage the whole device.
3) The stored data in the device need to be secure while moving from environment to another.
4) Administration of the security rules specially in PDA environment.
5) Connecting the device to public wireless networks creates high risks as many users connect to the same network without any authentication or encryption [7].

IV. Proposed Solution

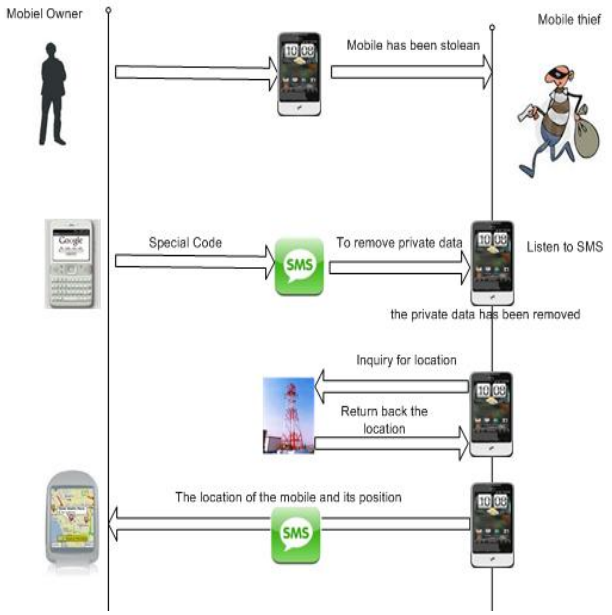

Fig. 1. Proposed solution for securing application in mobile computing.

After a thorough review of referenced literature, we now have clear vision of what is required to assess the state of security in mobile computing applications.

The main motivation of this exercise is to come up with a mechanism to ensure user's private data is protected and secured in the event of a mobile device being lost or stolen

In order to achieve this goal, following requirements have been identified, and will be addressed by the proposed solution:

1) Enable mobile device (phone) to receive SMS message with instruction codes to perform required operations to ensure private data is not misused.
2) Enable mobile device (phone) to broadcast its location and any other events to a given control number.
3) By enabling mobile devices to receive instructions via SMS messages, we will be able to lock the private data held on the phone such as:
   - Contact list
   - SMS, MMS
   - Call log
   - All Media files

The SMS command will be only accepted in a specific format and according to pre-configured specifications. This specification will be set up on the client as a part of the application configuration. The client device will only react on the SMS message command in the configured format in order to avoid any misuse by unauthorized users.

Moreover, the client application intercept the message before stored in the SMS inbox and start doing the necessary action to secure the application and private data.

The application can be configured to send available data to the control number such as Location Based Services data, etc. This data would depend on what is available on the device.

The SMS listening application and the broadcast client be written in Java using available mobile device APIs.

We have chosen Java over native programming languages in order to bypass any particular platforms OS or hardware advantages. By using Java we will ensure that each platform is using the same library.

The solution should be as light weight as possible in order to avoid consuming too many mobile device resources. This is especially important when intercepting and interpreting incoming SMS messages.

Our secure application in mobile computing works in two scenarios as the following:

First scenario when the thief does not change the SIM card (the secondary phone number does not receive a SMS with a new phone number). Then the phone owner of the stolen phone will send SMS with specific predefined format to his stolen phone number to do the necessary action (delete his private data, send to the secondary phone the location information with Latitude and longitude of the stolen phone).

Second scenario, when the thief changes the SIM card after stolen the phone.

In this case, the application should read the phone number in the current SIM card and compare it with the previous phone number in previous SIM card, if it is different from what is stored, the application will immediately send SMS to the secondary phone number with the information about the new phone number in the current SIM card. Hence, the mobile owner will send a SMS with specific predefined format to the new phone which was sent by the application earlier to do the necessary action (delete its private data, send to the secondary phone the location information with Latitude and longitude of the stolen phone).

A. Security Architecture

Android OS is a multi-process, each application runs in its own process. So ,the majority of the security between applications level and the system level is forced at the process level during standard Linux services, like group ID and user concept that are assigned to the applications. Android is designed by default as security architecture to each application that will not allow permission to do anything that affects other application, the operating system or users. This include the permission for reading and writing to the user private data (i.e. Contact- SMS) or access to the network..Etc. In order to develop the proposed solution and to achieve our target, we have to grant the application some permission to access the network and to write on the user private data such as contact, SMS. Etc.

B. Application Components

The proposed solution has the following main components:

1) Defense activity

It is GUI component to interact with the end-user. It provides interface to specify the following:

1) Emergency phone number field (your second phone number). It will be used to send SMS in case of SIM is changed or device is stolen.
2) Incoming emergency SMS format field. It is used for getting commands from the end-user from a different phone. Format should be like *DIGITS# (*123# for example). Specifying of optional codes is also possible. In this case the format should be same as above, but incoming SMS should looks like *DIGITS*OPCODE# (*123*1#).

2) SMS receiver

Actually, it is broadcast receiver to get Android broadcasts about incoming SMS. It executes the commands, which are extracted from incoming SMS. In case of base type of SMS it destroys all private user data (in case of device is theft) and sends back the device location. For the other SMS types, it executes the optional SMS codes. At present the next optional codes are supported:

1) *DIGITS*1#. By this code current device location is sent back to the emergency number. Obviously this set of optional codes can be expanded in the future.
2) Boot Completed Receiver.
3) Broadcast receiver for getting 'boot complete' Android events to start the Validity Service at boot time is completed.

3) Validity service

It starts at boot time and checks the SIM status. If SIM was changed from last time it sends SMS to emergency number about this fact. Additionally, Validity Service determines current device location. Android platform implements two Content Providers to determine location: Network Provider and GPS provider. Network Provider gets the location information directly from network operator. GPS provider gets the location information from GPS receiver. Validity Service subscribes to location changed events from both these providers.

By incoming location events from providers the validity service puts the location information to shared memory for using by SMS Receiver later.

C. Get Location Mechanism

Android platform use Network and GPS information to get current device location using Location Manager.

The cell phone operator provides the location information by network. It might or might not be available. This information is part of configuration traffic from operator in CDMA/GSM standards.

GPS location is provided by GPS receiver. In both cases, it takes some time (few minutes) to start getting updates from these two sources.

The validity Service subscribes to location updates from both providers as Network as well as GPS.

Every update is stored into the shared preferences of the application. On the other hand, SmsReceiver reads this information by incoming SMS if necessary and send as outgoing SMS.

If the location information is still unavailable in the shared preferences, SMS Receiver starts separate thread and waits this info up to 500sec. This period should be enough to GPS and Network providers are ready.

D. Development Environment

We have tried to select the suitable environment to achieve the targets and goals to do this type of project that requires special API, security permission and access.

The following are the list of components of the environment that used to develop this project:

1) Java development kit. It is possible to use JDK5 or JDK6.
2) Android SDK. The latest SDKs support all known platform versions that can be used for the development. It is online installer with GUI for settings.
3) Eclipse IDE is recommended by Google for the development under Android platform.
4) Additionally Android Development Tools (ADT) should be installed as Eclipse plug-in to provide Android projects support. It is installed as a plug-in using Eclipse.

V. Conclusions

In this work, we proposed a solution for mobile users to secure their applications and their sensitive data. The proposed solution is a mechanism to ensure user's private data is protected and secured in case of mobile device is lost or stolen that is based on Android operating system platform using Java language. The proposed application provides simple and flexible way to secure applications exists in the mobile device and their sensitive data.

Many security solutions do not meet complete security requirements in mobile devices. Securing mobile computing applications will remain an active research and development area [8].

Acknowledgment

I would like to take this opportunity to express our deep sense of gratitude and profound feeling of admiration of my supervisor Dr. Iehab Al-Rassan.

References

[1] C. R. Mulliner , "Security of Smart Phones," M.Sc. thesis, University of California, Santa Barbara, CA, 2006.
[2] W. Jansen and K. Scarfone, "Guidelines on Cell Phone and PDA Security," *Recommendations of the National Institute of Standards and Technology*, October 2008.
[3] A bitHeads. Mobile Application Development the Challenges and Best Practices. (2009). [Online]. Available: www.bic-innovation.com/knowledge/download/115
[4] B. Filho, R. Braga, W. Viana, and R. Andrade, "FRAMESEC: a FRAMEwork for the application development with end to-end SECurity provision in the mobile computing environment," *Advanced Industrial Conference on Telecommunications*, pp. 72-77, Lisbon, Portugal : AICT, July 2005.
[5] Mobile application development. (2011). [Online]. Available: http://en.wikipedia.org/wiki/Mobile_application_development
[6] Richard Aufrieter**,** "Mobile Security — New Needs on New Devices," *Network Security*, vol. 2002, issue 8, pp. 13-14, Sep 2002.

[7] W. K. Itani, "J2ME End-to-End Security for M-Commerce," *Wireless Communications and Networking, IEEE*, vol 3, pp. 2015 -2020, New Orleans, LA, USA : WCNC , March 2003.
[8] D. P. Agrawal, H. Deng, R. Poosarla, and S. Sanyal, "Secure Mobile Computing," *The 5th International Workshop on Distributed Computing IWDC 2003*, pp. 265-278, Kolkata, India, Dec. 2003.

Iehab Al-Rassan received his Ph.D. in Computer Science from the George Washington University. He has more than 20 years of experience in the field of IT, held many lectures and published many papers and articles in this field. His research interests include coding theories, information retrieval, string-matching algorithms, data compression, Business Process Management (BPM), distributed systems and handheld computing.