Remote Access and Protection of Smartphones using Short Message Service

Madhukumar GM, Sandeep karnam

Abstract—the smartphone usage among individuals is increasing quickly. With the exceptional growth of smartphone use, smartphone stealing is additionally increasing. This paper proposes a model to secure smartphones from stealing as well as provides choices to access a smartphone through alternative smartphone or a traditional mobile via Short Message Service. This model provides choice to track and secure the mobile by lockup it. It provides facilities to receive the incoming call and SMS information to the remotely connected device and permits the remote user to normalize the mobile through SMS. The projected model is valid by the standard implementation in Android platform.

Index Terms— Smartphone security, Remote access, Theft protection, Mobilephone security,

1 INTRODUCTION

THE Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal information now stored on smartphones. More and more users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

According to ABI Research the Mobile Security Services market will total around $1.98 billion by the end of 2014. All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, Wi-Fi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users. Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

- *Madhukumar GM is currently pursuing masters degree program in computer science in Jain global campus,Jain University, India, PH-+919164980031. E-mail: madhukumargm31@gmail.com*
- *Sandeep karnam is currently pursuing asst. professor in Jain global campus ,Jain University, India, PH-+917259332917. E-mail: karnam.sandeep@gmail.com*

Nowadays, usage of mobile has become a vital part of day-to-day activities of people. We can refer the current time as the era of Smartphones. Suppressing all other traditional communication purpose, smartphones are now at the peak of popularity in their usage of accessing the internet which includes mail access, social networking, mobile shopping and mobile banking. Smartphone usage of people is studied. Smartphones contains critical and sensitive data of user like automated call records, photos, videos and saved passwords of Web Pages. So losing the smart phone means a very high amount of irrecoverable data loss which may not be affordable in many cases. Few surveys about mobile theft in various countries have been studied.

This claims the need of an intelligent application to be run in mobile to eradicate mobile theft and track the mobile even after change of the SIM also. On the other hand, remote accessing of mobile becomes necessary when the mobile is left in somewhere like house or office. It includes getting the incoming call numbers, incoming messages, accessing call logs, changing phone's GPS, WIFI and profile settings and retrieving of contacts.

The major objective of proposed work has been listed below.

- Erase the essential information that has been keep within the mobile.
- We can locate and track the mobile using the proposed approach.
- Listen incoming calls and alert the remote device: The calls to the mobiles are frequently traced from a far off location.
- Listen incoming SMS and provides automatic reply and/or forward to remote user: Similar to tracking calls the Short Messages may also be tracked.
- Access and alter GPS, LAN, Data connection and profile settings through SMS.

2 RELATED WORKS

Shabtai et al. [1] provide a security assessment of the Android framework. Various threats may happen by exploiting vulnerabilities in the Android framework to harm, disable, or abuse confidentiality, availability, or integrity of the following Android assets: private/confidential content stored on the device (pictures, contacts, email, documents, and so on); applications and services (phone and SMS applications, Internet, and email); resources such as battery power, communication, memory, and processing power (CPU); and hardware, including the device itself, external memory cards, the battery, and the camera.

Benats et al. [2] also point out two shortcomings of privacy management in Android platform. First, Android's permissions system allows applications to call each other and under certain conditions one application can make use of any permission that was granted to another application. Second, there is no support for checking conflicts inside the resulting privacy permissions. Then they extend the privacy-aware role based access control (P-RBAC) [3] model to tackle this.

Delac et al. [4] illustrate a permission based security model to address security issues. This model is based on application isolation in a sandbox environment [5]. This means that each application executes in its own environment and is unable to influence or modify execution of other application.

In [6], an Android-based prototype that implements five collection techniques (Log cat monitoring, Broadcast Intent monitoring, Event Listener monitoring, application level collection, and operation data based generation) and a selective encryption function to protect sensitive data in the local database is developed. It encrypts parts of operation data for the balance of performance and security.

Gil et al. propose multi sensor architecture to obtain people context from smartphones [12] and Castillejo et al. introduce an Internet of things approach for managing smart services [13].
Rowaihy proposes location privacy in sensor allocation systems [14]. However, none of these works mentioned above use the simple way of SMS to protect users' privacy based on the Android framework.

3 PROPOSED SCHEME

The proposed scheme has two components. One is server component that is devoted to run in the smartphone which has to be accessed and protected. Another one is client component that would be in another smartphone to access the server component. In normal mobile phones, we cannot install the client component. In this case, the users will communicate directly through SMS. So the server has been designed to handle the request from the client component as well as the normal SMS command from the mobile phones.

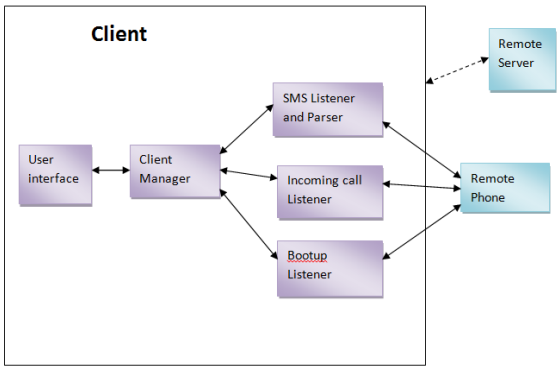

Figure 1: Architecture of Remote smartphone

The development starts from the client interface. To access a smartphone, the user should input the username, mobile number and the user defined remote connection password. This information will be converted by the client service and '$$' symbol will be added in the first two character of the message and sent to the server. In server side, after reading the first two characters, the service will decrypt the data to verify the authentication information.
Once the verification has been done, the server service will lock the mobile and display the login password. So, the mobile becomes inaccessible thus secured. After this process, the request from the client service will be responded and encrypted by the server and it will sent back to the client. The response will be decrypted in the client service and displayed in the client side. All SMS from client side to server will be followed by the '$$' symbol.

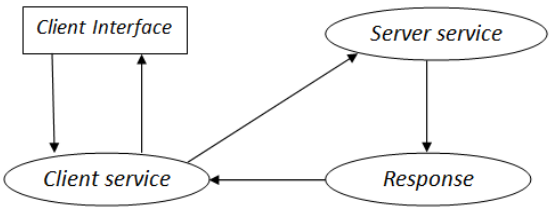

Figure 2: Overview of smartphone client.

If the user wants to access the smartphone from a normal mobile, the user has to message the '$' symbol followed by remote connection password from the mobile's messaging interface. Server service will differentiate the command from the smartphone's application and normal SMS by the first two character of the message. Depending on this, the response will be made. In this instance, response won't be encrypted and it will be sent back as a SMS to the user. Response can be the contact information stored the smartphone, an incoming call

number, and SMS stored in the device.

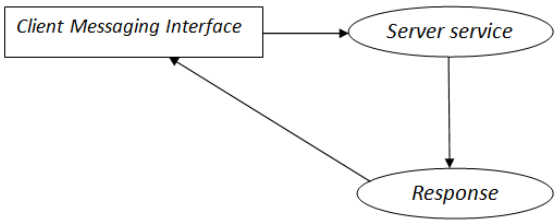

Figure 3: Overview of normal mobile client.

3.1 ALGORITHMS

The algorithms used in the proposed system are as follows:

Algorithm 1: Client component

This algorithm is used for client component.

Step1: Get mobile number and connection command from the user.
Step2: Encode it and add '$$' in the beginning and send it to remote number.
step3: Wait for authentication confirmation.
step4: Create login PIN for user to secure client interface and send it to user.
Step5: display client interface to user.

Algorithm 2: Server component

This algorithm is used for server component.

Step1: Receive incoming SMS
Step2: Check the command SMS and decrypt if it is encrypted.
step3: Check the database for remote connection status.
step4: If a remote connection is not established then check for authentication ,if it is an authenticated message then lock the mobile device and send to user and goto step 8.
Step5: Else check mobile number, if it is comes from authenticated mobile number then goto step 7 else goto step next step.
Step6: Implement SMS forwarding and automatic replay if it is enabled.
Step7: Wait for next incoming SMS.

Algorithm 3: Call Handler

Step1: Monitor the incoming call.
Step2: If new call arrives then get the number.
step3: check the call alert option in the database, if it enabled go to next step else stop.
step4: Send the call alert SMS with number to user.

4 EXPERIMENTAL ANALYSIS

Few tests were conducted in the implemented model. This helps to improve the model. To prevent misuse of the application, the model is updated with the following:

Number that failed to provide the correct authentication data will be added in the warning list for the first two attempts. This data will exist in the list for 48hours. Within 48 hours, if third attempt also fails, then the number will be added in permanent block list. Options provided to user to delete the list. During activate remote connection, if command comes from other number then remote user will be alerted and requested number will be added to block list immediately. Default application installation path is set to mobile storage so that wiping out of memory card won't affect the application. SMS parser is improved. It will detect request from mobile number exactly. Request from websites like way2sms will be rejected. Self-request to remote connection (client number is same as the server) will be rejected.

5 CONCLUSIONS

The proposed model has been implemented in android operating system. It was checked in Micromax A110Q smartphone. This provides the positive result. The model can be implemented in other smartphone platforms like windows, apple, etc. Accessing the mobile device from remote location using any other mobile device, SMS command received from the authenticated number will be sent to the server manager. There, the request handler will process the command and response will be made. Call handler will read the incoming call number and inform the client number by the call alert SMS if the call alert is activated. Mobile will be locked if the remote connection is active. Changing of SIM card in that smart phone will be detected by the boot up listener and will be informed to remote user if it so. Database handler will do all the read and write operation of the database. Mobile device used for accessing remote smartphone need not be an android device

REFERENCES

[1]. A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer,"Googleandroid:acomprehensivesecurityassessment," IEEE Security & Privacy, vol. 8, no. 2, pp. 35–44, 2010.

[2]. G. Benats, A. Bandara, Y. Yu, J.-N. Colin, and B. Nuseibeh, "PrimAndroid: privacy policy modelling and analysis for android applications," in Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY '11), pp. 129–132, Pisa, Italy, June 2011.

[3]. Q. Ni, E. Bertino, J. Lobo, and S. B. Calo, "Privacy-aware role- based access control," IEEE Security & Privacy, vol. 7, no. 4, pp. 35–43, 2009.

[4]. G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in Proceedings of the 34th International Convention on Information and Communication Technology,

[5]. Electronics and Microelectronics (MIPRO '11), pp. 1468–1473, Opatija, Croatia, May 2011. [5] "Sandbox," http://en.wikipedia.org/wiki/Sandbox (computer security).

[6]. K. Ohta, K. Kiminami, T. Nakagawa, C. Doi, and H. Inamura, "Design and implementation of privacy-enhanced operation history middleware for smartphones," in Proceedings of the 3rd International Conference on Ubiquitous and Future Networks (ICUFN '11), pp. 336–341, Dalian, China, June 2011.

[7]. G.B.Gil,A.Berlanga,andJ.M.Molina,"InContexto:multisen-sor architecture to obtain people context from smartphones," International Journal of Distributed Sensor Networks, vol. 2012, Article ID 758789, 15 pages, 2012.

[8]. P. Castillejo, J. F. Martinez, L. Lopez, and G. Rubio, "An internet of things approach for managing smart services provided by wearable devices," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 190813, 9 pages, 2013.

[9]. H. Rowaihy, "Location privacy and energy preservation in sensor allocation systems," International Journal of Distributed Sensor Networks, vol. 2012, Article ID 197592, 10 pages, 2012.