ISSN 2395-1621

Remote Security System For Smartphones

[#1]Mayuri Lingayat, [#2]Smruti Jadhav, [#3]Mayuri Shinde, [#4]Vinaya Sankpal

[2]smrutijadhav283@gmail.com
[3]shindemayuri66@gmail.com
[4]vinayasankpal@gmail.com

[#1234]Department of Computer Engineering, Zeal College of Engineering And Research,Narhe

ABSTRACT

The smartphone usage among people is increasing rapidly. With the phenomenal growth of smartphone use, smartphone theft is also increasing. If the phone is lost, then thief can misuse it and put user into deep trouble. The Propose System to secure and protect smartphones from theft as well as provides options to access a smartphone through other smartphone remotely or a normal mobile by using Short Message Service. This model also provides option to track and secure the mobile by locking it. It provides alarm system. There is an Android API which programmatically delete all data at a time. System in which we are taking backup of all important data, Such as images, files, contacts,sms,personal pocket etc.

***Keywords*:** Remote Lock and Wipe System, Smartphone's, SMS,Massage Authentication Code

ARTICLE INFO

Article History

Received 30th March 2016

Received in revised form :

1st March 2016

Accepted : 2nd April 2016

Published online :

4th April 2016

I. INTRODUCTION

Smartphone's are becoming more and more popular due to the increase in their processing power, mobility aspect and personal nature. Android is one of the most popular and fully customizable open source mobile platforms that come with a complete software stack.Main reasons behind the rapid growth in adoption of Smartphone are their capability to facilitate users with third-party applications. When user is absent or when phone is lost any person can misuse mobile data.Hence user want complete security in their absence. The locking of the android phone through the SMS is used to overcome the entire problem which they are facing currently and making the complete secure your android phone from anywhere and anytime.If your phone crashes unexpectedly, or worse gets lost or stolen, then you'll not just be down the cost of a phone, but also a huge amount of data. To get around that, you need to enable server backups for as many things as possible, so that logging your account into a server transfers most of your data automatically. Your phone contains more personal data than you may realize. Everything from your alarms to your text messages are evidence of your use habits, let alone private information. By backing up your phone, you not only ensure that your data is protected in the event of theft or damage, but also that you can make a smooth transition when upgrading devices.Note that Remote Wipe erases the device's internal storage. Your user's device must already have Device Policy configured.

II. RELATED WORK

A Survey on:Phone Protector: Protecting User Privacy On the Android-Based Mobile Platform.

The growing trend towards the Android platform basedmobile phones, privacy and security of Android platform becomes a very important. Nowprotection for Android based smart phone has many deficit,and most phone security systems are based on client-server model. In this paper a browser-freemultilevel smart phone security system, this is based on the Android sensor platform.In this system, protection is ensured by means of SMS. Users can send SMS to phones remotely as operating command. After that the sensors on remote phones run the command and return important information. Next is,the sensorsbased on the daemon process mechanism are used to forbid the sensors from being maliciously closed and uninstalled. Third system acquire SIM detecting mechanism to judge whether the SIM card is removed or changed. If exception is detected, the phone will be locked automatically by its

inside sensors.The three points ensure full protection of phone privacy.Results show that system has good robustness and low resource consumption.

A Model For Remote Access And Protection Of Smart Phones Using Short Message Service.

The smartphone usage among people is increasing day by day rapidly. With this phenomenal growth of smartphone use, smartphone stealing is also increasing. These papers introduce a model toprotect smartphonesagainst theft. This system provides options to access a smartphone through other smart-phone remotely or a normal mobile via Short Message Service. This modelalso provides option to track and secure the mobile phones by locking it. It also provides facilities to receive the incoming call and sms information to the remotely connected device and enables the remote user to control the mobile through SMS. The proposed system is validated by the prototype implementation in Android Base Platform.

Smart Phone For Mobile Commerce.

For the Companies it is necessary to meet customer's requirements that should always take into account new technological solutions, which are increasingly used by consumers. Technologies, which has become increasingly advanced and popular, is the smart phone. Today's smart phones have become a useful device for both various retail stores and customers. Customers can quickly search in their smart phones for the price of the product on proposeswebsites. These extensive capabilities of smart phones have led to a new kind of competition for traditional stores. On the other side retail stores can use smart phones in order to inform their customers about new promotions, new events, new technology etc. The main objective of this system is to introduce the scale and the reason of the use of smart phones by customers in traditional retailing. The system focused on smart phone utilization by customers at a time of shopping. As well as in this paper survey results have been presented, which had been conducted among smart phone users in one medium-sized city. The research results showing that cell telephony while shopping has yet to reach the same level of popularity among Polish customers, which it has attained in other countries.

III.EXISTING SYSTEM

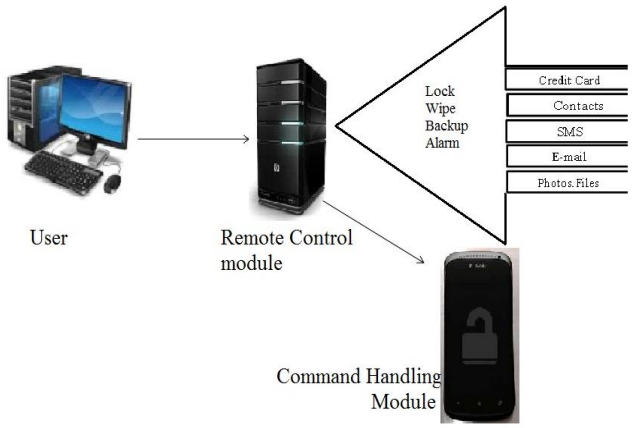
A. The Remote Lock And Wipe System

The system of remote lock and wipe system namely contains two modules. First one is remote controlmoduleand the second is command handling.The remote control module on a server side and the command handling module on a smartphone.Then the commands are sent by SMS push notification message. After that when the users send a lock command to the smartphone via the remote control module, the remote handling module enables the password locking function to lock the smartphoneremotely. Like that, by sending a wipe command, all personal data of user such as smart wallet, smart keys, contacts, SMS, E-mail, photos, and movie clips are deleted remotely.

B.Integrity Checking

Wipe system And Remote Lock using SMS push notification with integrity checking of the commands without loosing security level. In this System they employ password-based key derived function (PBKDF) in PKCS#5 which requires users to put only a password in and outputs 20 bytes long authentication code.

IV. PROPOSED SYSTEM

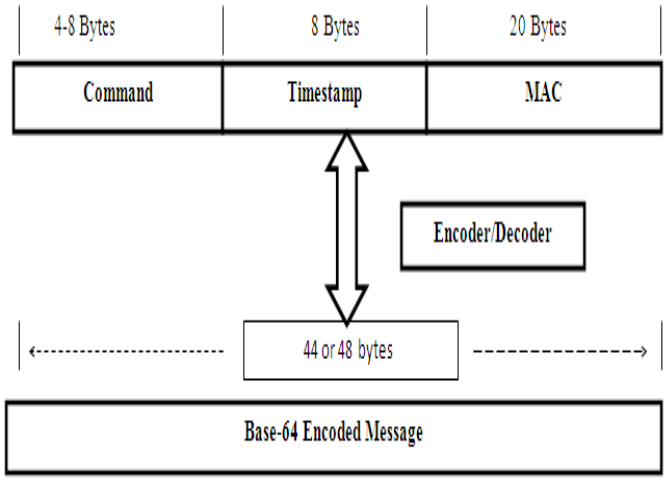


The system proposes remote lock and wipe system using SMS push notification And Integrity checking.System also provides backup of all important data as well as alarm system without sacrificing security level. Remote security system will consist of three modules user application, remote server, and tracking application.The server will be used for storing users info, storing their backup data, storing there location info.The SMS listener and parser in the server will receive all the incoming messages and check for the command in the SMS. In our proposed system command will be preceded by the for the smartphone client and it will be preceded by the formobile client. If the SMS starts with the then the characters of the SMS will be decrypted. Authentication to remote mobile number has been done by checking the user login command in the received message. Once the authentication has done, the mobile keypad and touch screen will be locked and the prompt for the login password will be asked to unlock the mobile. After this, 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. Boot handler will receive the mobile boot up so that the application will be started automatically when the mobile boots up. Mobile will be locked if the remote connection is active. Changing of sim card in that smartphone 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.

A. SMS Command Handling Process

In the Propose system we employ password-based key derived function(PBKDF). System Uses Android broadcast receiver which will receive our all sms commands and match it with regex pattern that if tracking application has

sent it any command.when SMS command is sent remote control module create secret key using PBKDF, after that message authentication code is generated on command message.command message send to target smartphone. To send the message in the form of SMS sending message must be encoded with base-64. So the system will use base64 encoding decoding to send command using message so that no one will understand the command in message box. By using Base-64 encoding system taking binary data and turning it into text so that it is more easily transmitted in thing.



V. ALGORITHMS

1.PBKDF(Password Based Key Derived Function) :- The PBKDF key derivation function has five input parameters:

$$DK = PBKDF2(PRF, Password, Salt, c, dkLen)$$

where:

- PRF is a pseudorandom function of two parameters with output length hLen (e.g.akeyed HMAC)
- Password is the master password fromwhich a derived key is generated
- Salt is a cryptographic salt
- c is the number of iterations desired
- dkLen is the desired length of the derivedkey
- DK is the generated derived key
- Each hLen-bit block Ti of derived key DK, is computed as follows:

$$DK = T1 \,||\, T2 \,||\, ... \,||\, Tdklen/hlen$$
$$Ti = F(Password, Salt, Iterations, i)$$

- The function F is the xor(^) of c iterations of chained PRFs. The first iteration of PRF uses Password as the PRF key and Salt concatenated with i encoded as a big-endian 32-bit integer. (Note that i is a 1-based index.) Subsequent iterations of PRF use Password as the PRF key and the output of the previous PRF computation as the salt:

$$F(Password, Salt, Iterations, i) = U1 \wedge U2 \wedge ... \wedge Uc$$

where:

$$U_1 = PRF(Password, Salt \,||\, INT\_msb(i))$$
$$U_2 = PRF(Password, U_1)$$
$$...$$
$$U_c = PRF(Password, U_{c-1})$$

2. MAC(Message Authentication code) :-
HMAC (K,m) = H((K ⊕opad) ‖H((K ⊕ipad)‖m))

Where

H is a cryptographic hash function, K is a secret key padded to the right with extra zeros to the input block size of the hash function, or the hash of the original key if it's longer than that block size, m is the message to be authenticated, ‖denotes concatenation, ⊕denotes exclusive or (XOR), opad is the outer padding (0x5c5c5c…5c5c, one-block long hexadecimal constant), and ipad is the inner padding (0x363636…3636, one-block long hexadecimal constant).

VI. IMPLEMENTATION

The proposed System is implemented in java 4.2 by using various package and functions. The command handling Module for smartphone is implemented on Android –SDK . While implementation the main performance requirement is recovery of data.

VII. CONCLUSION

The system proposes the mechanism to provide security to the user by using remote lock and wipe which protects the users data and prevents the malicious user from launching DoS attack that sends such commands to the normal users intentionally. Propose System also taking backup of all important data remotely. There is a provision policy in android where we write policy to lock device, unlock device , delete all data of phone. We will use base64 encoding decoding to send command.

REFERNCES

1. Kyungwhan Park1, Gun Il Ma1, Jeong Hyun Yi1, \Smartphone Remote Lock and Wipe
System with Integrity Checking of SMS Noti_cation", Member IEEE, Youngseob Cho2,
Sangrae Cho2, SungeunPark3 ,Soongsil University, 2Electronics and Telecommunications

Research Institute, 3KSIGN Corp., IEEE Transaction on Consumer Electronics (ICCE),
Vol 7, No.13, Sep 2014

2. Y.F. Chang, C.S. Chen, and H. Zhou, " Smart Phone For Mobile Commerce", Computer
Standards and Interfaces, Vol. 31, Issue 4, June, 2009

3. Sha_k G. Punfa and Richard P. Mislan, "Smartphone Device Analysis", Small Scale Digital
Device Forensics Journal, Vol. 2, No. 1, June, 2008.

4. Oracle, "http://download-llnw.oracle.com/javase/1.4.2/docs/api/javax/c-rypto/ package-
summary.html"

5. ,Weizhe Zhang,1Hui He,1 Qizhen Zhang,1 and Tai-hoon Kim2, \Phone Protector: Pro-
tecting User Privacy on the Android-Based Mobile Platform", International Journal of
Distributed Sensor Networks Volume 2014

6. K.S.Kuppusamy, Senthilraja R,G. Aghila," A model for remote access and protection of
smartphones using short message service", 2012

7. Y.F. Chang, C.S. Chen, and H. Zhou, "\Smart Phone For Mobile Commerce" ,2011

8. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC
Press, 1996

9. Kyungwhan Park, Gun Il Ma, 2.Jeong Hyun Yi, Youngseob Cho, Sangrae Cho, Sunge-
unPark, "Smartphone Remote Lock an d Wipe System with Integrity Checking of SMS
Noti_cation" ,ConsumerElectronics (ICCE), IEEE International Conference on 9-12 Jan.
2011.

10. Android SDK: http://developer.android.com/sdk/android-2.3.html

