ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Smartflage: Data Transfer among Different Modes for Mobile Android System

Sushil Kumar [(1)]; Sunil Kumar [(2)]

(1) University of Delhi, Shyamlal College Delhi, India
(2) University of Delhi, Institute of Informatics and Communication New Delhi, India

Manuscript Info

Manuscript History:

Received: 12 October 2015
Final Accepted: 25 November 2015
Published Online: December 2015

Key words:

Encryption,Decryption

Corresponding Author

Sushil Kumar

Abstract

The impact of Smartphone in our daily routine is increasing day by day. Due to emerging technologies protection of data is the mainissue. Encryption technique plays an important role in protection of data.There are several approaches to provide the security of data. When the data is communicated or stored then numerous scenarios i.e. security issues, quality of service etc could take place. In this paper we are going to develop an approach which provides thedata transfer among Administrative mode, User mode and Guest mode.

Copy Right, IJAR, 2015,. All rights reserved

INTRODUCTION

Smartphone is basically a mobile phone which is having an operating system [1][2][3]. Smartphoneusuallyhaving the configurations of a phone having admiredend user devices, i.e.Wireless Fidelity (Wi-Fi), third party application, motion sensor, payment using mobile. Reputation of Smartphone basically deals from their small size, complicateddevelopmentand ability of connection, low-priced, and their potential to congregationflexible third party applications. Dissimilar kinds of data are basically organized by the Smartphone i.e. login id for communication, consumption or creation of data by applications etc. Smartphone can be used for different purposes i.e. business and user based data. In the current scenario Smartphone is accepted worldwide. Due to vulnerable types of data, mostly mobile operating system has storage encryption space.

Different service providers use different types of encryption techniques i.e. Apple's iOS use file based and android uses full disk encryption. Android full disk encryption technique has the problem of deniable encryption i.e. if the user is forced to give decrypted key.

According to plausible deniable encryption, data is encrypted with different key but original can be recovered with the true key only. If the user is forced by the invader, then user provide the different key instead of true key to access the original data [3]. Some genuine real-world situation can permission the
employ of Plausible Deniable Encryption allowed storage .i.e. a human privileges employee working in a section of conflict. A terrorist who belongs to terrorist group enters into Australia by stitching the SD card which contains the evidence of slaughter, underneath his skin. Smart phones broadly utilized to detain and distribute numerous videos and images of popular revolutions etc.Plausible deniable encryption is used to avoid a user from being penalized in case of controversial stuff; an invader can impound the appliance itself if such type of data is supposed to survive [4].

In desktop operating system full disk encryption can be achieved with plausible deniable encryption scheme.
For desktop PC true crypt tool can be used. But for mobile operating systems there are no such types of tool.

Mobile devices most widely used by the users in comparison to laptop and desktop PCs. Smartphone .i.e. android operating system provide the framework for encryption and decryption with the help of soft keyboard. Desktop or laptop windows use true crypt boot loader. Plausible deniable encryption system .i.e. Mobiflage contains all the recognized attacks adjacent to desktop PCs [5].Mobiflage basically a plausible deniable enabled storage encryption system which only support Android operating system. Plausible deniable encryption technique lacks in the sense that if user provide the true key by mistake to decrypt the data.

The worldwide sales of mobile devices, especially forsmartphones, grew by an increasing rate over the last years.Gartner says that 304 millions of mobile device units wheresold in the year 2010, which is an increase of 72.1 percent incomparison to the year 2009 [1]. The increasing popularity andcapability of mobile devices and the confides of organization to integrate them into their business processes represents anattractive target for criminals to attack [2]. As a consequence,organisations need to implement policies to manage the risk ofusing mobile devices in an enterprise environment, especiallywhen the data that the mobile devices are handing is sensitiveand confidential.

Smartphonereputation lies primarily from their tiny size, sophisticated processing and connectivity capabilities, cheapprice, and their capability to host versatile third party appliances. Smartphoneorganize differenttypes of data .i.e.communication logs, data created or consumed by applications, sensor data and multimedia etc. In spite of not being secure, Smartphone users take away the device on different location and used with different network connectivity. Smartphone is used as multipurpose device .i.e. personal and business oriented data. Now a day's Mobile computing devices and Smartphone are being extensively adoptedworldwide. Due to increasing number of users day by day i.e. 1.75billion Smartphone users worldwide as per emarketer.com report [1] [2], the amount of individual data accumulated in Smartphone has also been augmented.Mostly mobile operating system producers presently containsome point of storage encryption due to susceptible nature of data. Different service providers use different types of encryption techniques i.e. Apple's iOS use file based and android uses full disk encryption. Android full disk encryption technique has the problem of deniable encryption i.e. if the user is forced to give decrypted key.

According to plausible deniable encryption, data is encrypted with different key but original can be recovered with the true key only. If the user is forced bythe invader, then user provide the different key instead of true key to access the original data [3]. Some genuine real-world situation can permission the

employ of Plausible Deniable Encryption allowed storage .i.e. a human privileges employee working in a section of conflict. A terrorist who belongs to Islamic state enters into Australia by stitching the SD card which contains the evidence of slaughter, underneath his skin. Smart phones broadly utilized to detain and distribute numerous videos and images of popular revolutions etc.Plausible deniable encryption is used to avoid a user from being penalized in case of controversial stuff; an invader can impound the appliance itself if such type of data is supposed to survive [4].

In desktop operating system full disk encryption can be achieved with plausible deniable encryption scheme. For desktop PC true crypt tool can be used. But for mobile operating systems there are no such types of tool. Mobile devices most widely used by the users in comparison to laptop and desktop PCs. Smartphone .i.e. android operating system provide the framework for encryption and decryption with the help of soft keyboard. Desktop or laptop windows use true crypt boot loader. Plausible deniable encryption system .i.e. Mobiflage contains all the recognized attacks adjacent to desktop PCs [5].Mobiflage basically a plausible deniable enabled storage encryption system which only support Android operating system. Plausible deniable encryption technique lacks in the sense that if user provide the true key by mistake to decrypt the data. To tackle such issue we are designing a system called Smartflage:

I. BACKGROUND

In the following section, we have argued Smartflage'shazard model and equippedhypothesis, and few legal features of using true crypt in general. The mainanxiety with upholding whether the system will provide any clue of the continuation of someunknown data.Smartflage'shazard model and hypothesizes are mostly based on past work on mobiflage [6].

1. Smartflage must be merged with the default Android code stream to ensure that many devices are capable of using true crypt. After that an opponentwill be incapable to crafthypothesis about the existence of concealed volumes based on the accessibility of softwaresupport.
2. Smartflagepresentlyneeds a material Static Digital card. Devices i.e. Galaxy Nexus does not support external storage but it basically uses the media transfer protocol and split a single partition for the internal application storage and external user reachable storage. This external reachable storage is further divided into internal and

external storage. Theinvader has the knowledge of the device which is already encryptedas well as complete knowledge of Smartflage's design, but don't have the encrypted key and the matching password. The offset of Smartflage'shidden volume is reliant on the password of true crypt. So invader doesn't have the knowledge about it.

3. The invader can forced the user to disclose their encryption keys and passwords i.e. unlock screen secret but invader will be able to get the true key. To disclose the original data true key is needed. But if by chance user had provided the true key to the invader then data will be lost. To avoid this problem Smartflage provide the deniability by encrypting and hide and again encrypting and hide the data. So user had to enter true key two times. Theinvader can also have right to use the device internally as well as externally and so invader could access complete storage from root level. Invader can manipulate the disk by dictionary attack. Such type of problem can be tackle with Smartflage [8].
4. In case of desktop, invader periodically access the encrypted volume [9, 1] on the other hand for mobile devices invader need to access the storage volume only after the detaining the user. Invadercan gather service action logins from carriers to disclose the use of an encryption mode on alleged devices. This hypothesis significantly fortifies the invadermodel [8].
5. It is assumed that mobile operating system, boot loader and kernel are free from malware. If invader has the access to operating system then invader can invader can intercept data and monitor the ongoing call [5].It is also assume that invader don'tdetain the user device while in the encrypted mode. User has to follow the certain guidelines i.e. user has to use the device in administrative, user as well as guest mode periodically.

III. PROPOSED WORK

In this section, we mainlyexplainspecificselectionsthat areaccomplished for Smartflage.We discriminate between the recommendedobjectivesof SmartflageSecure digital and Smartflage media transfer protocol. All the proposed components are explicit to the android.Android is basically implemented as prototype. It is intended that most of the features are distracted to other systems.

We have basically createdthreecloselevels: an administrative level forsettings and applications, and a biggeradditionallevel todocuments, photosetc. We describe the subsequentapproaches of operation forSmartflage [15].

a) **Administrative mode:**In this mode of operationdatais stored secretly and if invader wants to access this data could not access. True password is only provided during the entering mode of operation. Secret data is stored at the same place where the physical storage takes place in the normal way. Invader can easily detect the composition of data after decrypting the extra storage space.If extra space is not available for the storage of data in that case an invader could easy guess that there would be secret data. In the data is encrypted two times using two different keys i.e. true key 1 and true key 2 [16] [17].
b) **User'smode:**In this mode user performs activities for everyday. It is the default mode and data is stored by default in this mode.Without any difficulty storage encryption is performed. Password is entered at the time of booting.
c) **Guest mode:**In this mode only a user other than particular organization can access the mode i.e. guest access the device.

If in a case when it is necessary to transfer of data without switching the modes i.e. if user don't have enough time for switching.We are offering asafe mechanismfor transferring data among several modes i.e. Administrative mode, Guest Mode, User mode. We basically build up both the volumes concurrently which provide the simple solution but we have to compromise regarding security issue. Because sensitive files can be transferred to the secured space [10-14].

IV. CONCLUSION

Mobile devices are increasingly being used for capturing andspreading images of popular uprisings and civil disobedience.To keep such records hidden from authorities, deniablestorage encryption may offer a viable technical solution.

Such PDE-enabled storage systems exist for mainstreamdesktop/laptop operating systems. With Mobiflage, weexplore design and implementation challenges of PDE formobile devices, which may be more useful to regular usersand human rights activists. Mobiflage's design is partlybased on the lessons learned from known attacks and weaknesses

of desktop PDE solutions. We also consider uniquechallenges in the mobile environment (such as ISP or wirelesscarrier collusion with the adversary). To address someof these challenges, we need the user to comply with

certainrequirements. We compiled a list of rules the user must followto prevent leakage of information that may weaken deniability.Even if users follow all these guidelines, we do notclaim that Mobiflage's design is completely safe against anyleaks (cf. [7]). We want to avoid giving any false sense ofsecurity. We present Mobiflage here to encourage furtherinvestigation of PDE-enabled mobile systems. Source codeof our prototype implementation is available on request.

REFERENCES

[1]. S. Calcote, Developing a secure health-care information network on the internet, Healthc. Financial Management, 1997, p. 68.
[2]. C.P. Pfleeger, Security in computing, 2nd ed.,Prentice-Hall International Inc., USA, p. 574,1997.
[3]. G. Carter, A. Clark, E. Dawson, L. Nielsen, Analysis of DES Double Key Mode, In: Proceedings of the IFIP TC11 eleventh international conference on information security, Chapman and Hall, UK, 1995, p. 13–127.
[4]. IDEA encryption. http///xfactor.wpi.edu:Works: MQP:securenet:root:node32.html
[5]. The risks of key recovery, key escrow, and trustedthird party encryption. http///:www.crypto.com:key-study.txt
[6]. Response to DTI Proposals on TTP Encryption Services. http:::www.r-cube.co.uk:dtiresponse.html.
[7]. Android, "Device administration." [Online]. Available:http://developer.android.com/guide/topics/admin/device-admin.html.
[8]. Android, "Google apps for enterprise: Device policy fr android: bersichtfrnutzer." [Online]. Available:http://www.google.com/support/mobile/bin/answer.py?answer=190930x.
[9]. D. Dolev and A.C. Yao, "On the Security of Public Key Protocols,"IEEE Trans. Information Theory, vol. IT-29, no. 2, pp. 198-208, Mar.1983.
[10]. R.-P. Weinmann, "Baseband Attacks: Remote Exploitation ofMemory Corruptions in CellularProtocol Stacks," Proc. USENIXWorkshop Offensive Technologies (WOOT '12), 2012.
[11]. TheRegister.co.uk, "UK Jails Schizophrenic for Refusal to DecryptFiles," News Article, http://www.theregister.co.uk/2009/11/24/ripa_jfl/, Nov. 2009.
[12]. TheRegister.co.uk, "Youth Jailed for Not Handing OverEncryption Password," News Article,http://www.theregister.co.uk/2010/10/06/jail_password_ripa/, Oct. 2010.
[13]. A. Hoog, Android Forensics: Investigation, Analysis, and Mobile Securityfor Google Android. Elsevier, June 2011.
[14]. S. Lee, K. Fleming, J. Park, K. Ha, A. Caulfield, S. Swanson, Arvind,and J. Kim, "BlueSSD: An open platform for cross-layer experimentsfor NAND flash-based SSDs," in Proc. Int. Workshop Archit. Res.Prototyping, Jun. 2010.
[15]. J. R. Douceur and W. J. Bolosky, "A large-scale study of file system contents," in Proc. Int. Conf. Measur. Model. Comput. Syst.Jun. 1999, pp. 59–70.
[16]. H. Huang, W. Hung, and K. G. Shin, "FS2: Dynamic data replication in free disk space for improving disk performance and energy consumption," in Proc. Symp. Operating Syst. Principles, Oct. 2005,pp. 263–276.