ISSN 22773061

AFDroid: Anti-Forensics Device To Protect Android System

Ahmad Talha Siddiqui[1], Shoeb Ahad Siddiqui[2], Mohammad Ibrahim[3]
Research Scholar IFTM University, Moradabad
ahmadtalha2007@gmail.com
Assistant Professor, Department of Computer Science, Integral University
siddiqui.shoeb3@gmail.com
M.Tech (CS), Al-Falah School of Engineering and Technology
ibrahimd35@gmail.com

Abstract

Mobile devices are among the most common new technologies of the year, gaining even more spread over and success in the day-to-day life of wide range of people. Unfortunately, while the number of mobile devices are used in crime activities is spreading and growing all over the world, the capability to perform the forensics analysis of such devices is limited both by technological and methodological problems. In this paper, we focus on anti forensics techniques applied to mobile device. Furthermore we observe the effectiveness of techniques.

Keywords

Android, Anti-Forensics, Mobile Devices.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol 9, No 3

editor@cirworld.com
www.cirworld.com, member.cirworld.com

1. Introduction

Mobile devices and particularly Smartphone are among the most common and overspread current technologies. There are billions of subscribers in the world and the modern trend of growth who have registered especially in the rural areas, confirms that this technology is overspread. In addition to the market penetration of such devices, another interesting item is also represented by the advanced functionalities which they already have. These functionalities range is from user interface to computational resource to connect an application development. Now there is possibility of categorizing three different classes of mobile phone basic, advanced and smart.

During the development from basic to smart phones, the amount and kind of personal data in simple phonebooks and text messages in basic phones, developed to a complex and wide set of personal information(e.g multimedia and email messages), browser of Anti Forensic techniques are evolving continuously and rapidly.

In this paper are give attention to anti forensic in any attempts to compromise the availabilities or usefulness of evidence in the forensic process. The availability of the evidence can be compromised by presenting its creation, by manipulating as well; and also its usefulness can be compromised by deleting the evidence or by tampering its integrity. This paper is divided into different sections: Section 1 introduction to Mobile Device. Section 2 deals with a general definition of Anti Forensic and its techniques. Section 3 deals with a brief description of Android Operating System, with particular attention to the Anti Forensics techniques. Section 4 deals with device administration. Section 5 describes the instance, to Android device of such techniques.

2. Kind of Anti Forensics

In this paper kind of AF techniques were described in arriving at an anti forensics consensus. These techniques have been identified in general, and are briefly summarized as follows:

1. Destroying evidence
2. Hiding evidence

2.1 Destroying evidence

It involves in the destruction of evidence, in order to make its unusable during the investigative process, although the destruction of history role of network accounts, application data, internet and many more in smart phones.

Last Year, a new and strong alarming trend was discovered by the forensics investigators, the uptick in the use of anti forensics. Currently such trends seem to be confirmed in the classic forensics environments. But in the near future, it could become interesting for smart phone forensics as well. The work presented in the paper focuses on the instance of some common Anti-Forensics techniques to android mobile device.

Anti-Forensics is a quite young and in mature discipline even more if we give attention to the mobile environment, concerning to mobile environment, there are so many difficulties and issues during forensics are still to overcome. Therefore the possible shapes evidence is often fatal. OE noticing that the tools or the operations used to destroy the evidence can produce evidence themselves in terms of trace of their usage.

2.2. Hiding evidence

Action taken to destroy the power and influence of the analyst rather than a specific forensic analysis application to decrease or even nullify the visibility of the evidence during the forensics analysis. The strength of this techniques is strictly connected to the limitation of the people or if any of the used forensics tools. Therefore the presence of any hiding tools can generate evidence.

2.3. Mobile anti forensics

We have given a light on mobile forensics with the related implication on the kind of digital evidence in which we are interested. In their year, due to the storage of the rich amount of personal information mobile devices became more important in forensics field but the classical forensics guideline and tools are not suitable for MDs as well. Probably the unavailability of a direct access to the internal memory of such devices is the main impediment to overcome. In fact if the external storage volume can be separated from the device and analyzed in a straight forward manner, but the internal memory volume cannot analyzed like that.

3. The android operating system

Android is a set of open source software elements specially designed for MDs developed by Google; it includes the operating system, a middleware and a set of application. Although it has been designed and developed for MDs (e.g., Smartphone), several laptop manufactures plan to equip their product with Android. Android will be second Operating System, behind Symbian, in term of Smartphone's market.

3.1. Android File System

Android is the natively supported YAFFS2 file system another interesting element of android. YAFFS stands for yet another Flash FS; it is the only FS that has been specifically designed for NAND flash chips. The use of NAND flash chips in the field of embedded and mobile devices in increasing and replacing the common old NOR chips because of the improved density, speed and reduced cost: YAFFS was released in two version:

YAFFS1: designed for old NAND chips with 512 byte pages plus 16 byte spare areas.

YAFFS2: evolved from FAFFS1 to accommodate newer chips with 2048 byte pages plus 64 bytes spare areas.

In addition to the different NAND chips supported YAFFS2 supported to the write once requirement modern NAND flash and evolved in term of performance, reliability and efficiency.

3.2. Applications and sandboxes

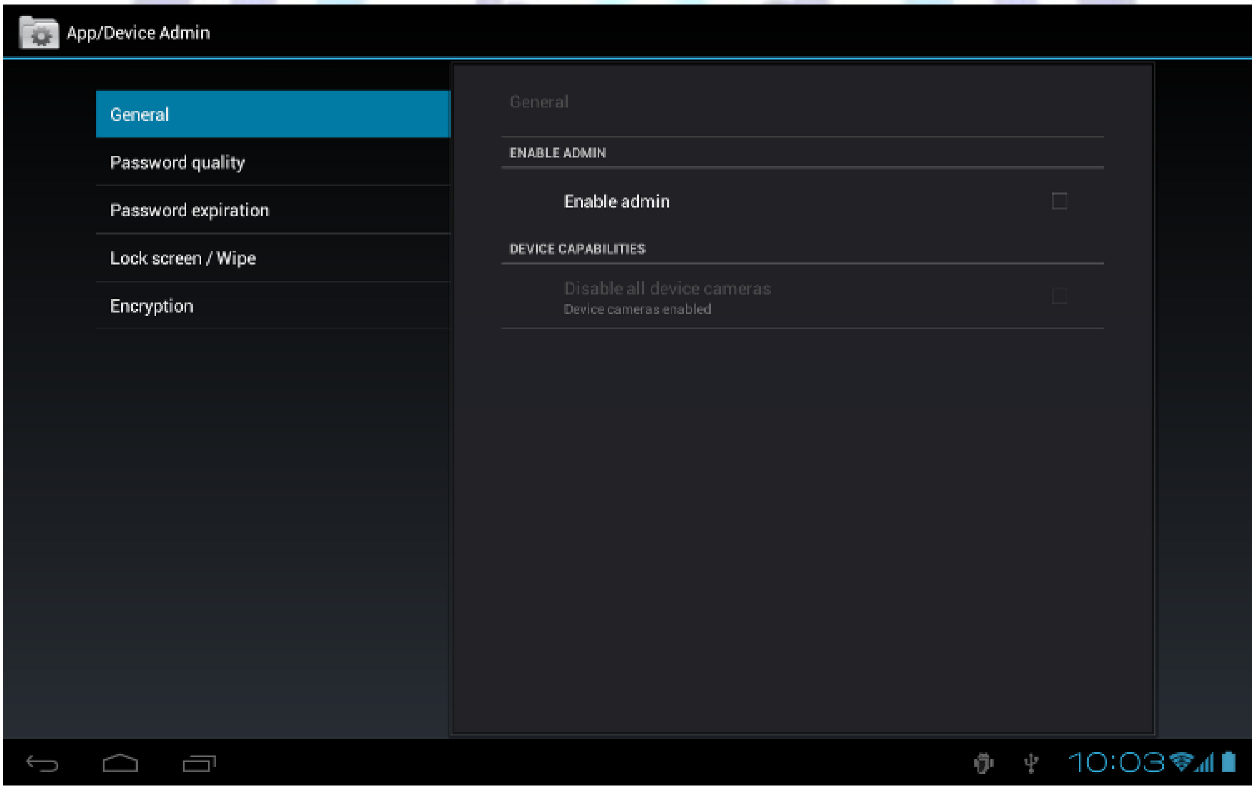
Android by default, devices to any application the capability to perform operations with the objective to hamper any other application the OS or the end-user. Hence, due to this design for applications it is impossible to perform any operation to end-user.

3.3. User IDs and permission

Android manages each installed application as a different LINUX user, at installation time, any application is provided with its own unique LINUX user ID. All the data stored by a given application will receive the application's user ID to grant to other applications any access to such data.

4. Device Administration

Android introduce support for enterprise applications by offering the ANDROID Device administration API; Device administration features at the system level is provided by the device administration API. These APIs also allow us to create security aware applications that are useful in enterprise setting. After the tremendous growth in Android email application has leveraged the new APIs to improve exchange support. Device administrators can enforce password policies including alphanumeric passwords or numeric pins-across devices through the applications. It discusses the various features provided by the Device Administration API to provide stronger security for employee devices that are powered by Android.



Enable admin □

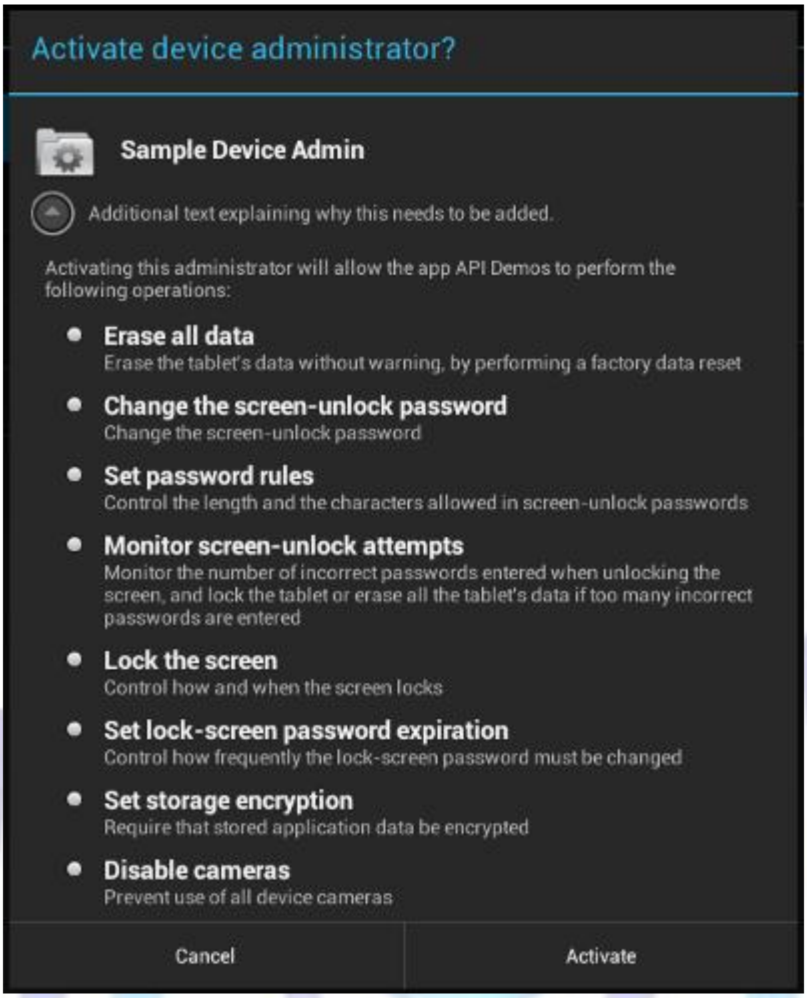
Disable all device cameras □
Device cameras enabled

Figure 1. Screenshot of the Sample Application

4.1 Enabling the Application

One of the major events a device admin application has to handle is the user enabling the application. The user must explicitly enable the application for the policies to be enforced. The process of enabling the application begins when the user performs an action that triggers the ACTION_ADD_DEVICE_ADMIN intent.

When the user clicks the **Enable Admin** checkbox, the display changes to prompt the user to activate the device admin application, as shown in figure 2:



Activate device administrator?

Sample Device Admin

Additional text explaining why this needs to be added.

Activating this administrator will allow the app API Demos to perform the following operations:

- **Erase all data**
  Erase the tablet's data without warning, by performing a factory data reset
- **Change the screen-unlock password**
  Change the screen-unlock password
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords entered when unlocking the screen, and lock the tablet or erase all the tablet's data if too many incorrect passwords are entered
- **Lock the screen**
  Control how and when the screen locks
- **Set lock-screen password expiration**
  Control how frequently the lock-screen password must be changed
- **Set storage encryption**
  Require that stored application data be encrypted
- **Disable cameras**
  Prevent use of all device cameras

Figure 2. Sample Application: Activating the Application

5. Android Anti Forensics Techniques and Tools

In arriving at an anti forensics consensus there is some of the possible instance of the AF techniques that have been identified. It is worth to matching that there instances do not represent a comprehensive set of all the possible techniques it is worth to noticing that these instance do not represent a comprehensive set of all the possible techniques that can be implemented.

5.1. Android Debug Bridge (ADB)

Android debug bridge is a tool provided such that android SDK which allows the interaction between the mobile device and a remote work station. ADB allows the remote execution of commands onto the mobile device; if the device is the enumerator, or if it has been rooted the commands are extended with the root privileges, otherwise they are strictly limited.

5.2. NANDROID Backup

Nandroid (tool) restore capabilities for rooted android devices and it is a set of tools supporting the backup. Nandroid also support the full NAND flash memory imaging which can be performed by a special boot mode.

5.3. Commercial Tools

If the availability of both commercial and free tools has been a contentions item. For mobile forensics this phenomenon is true. There are several major manufacturers of commercial tools in the market which are in competition from those some are to support or plan to support android mobile device.

5.4. AFDroid

It is observed that all the following techniques have been implemented by a common Android application that can be installed and executed onto the device; such application is called AFDroid

5.3. Android Destroying Evidence

This technique has been applied to text message, to the browser bookmarker and to the call log, in order to delete from the related data base any records carrying sensitive information. The deletion of such records and the secret storage performed by the private folder is a suitable example of evidence destruction.

6. Conclusion

Anti-forensic is a quite new and recently buildup discipline, especially when come to the account of mobile environment several efforts steps and efforts have been taken in order to properly describe and classify the widespread Anti-forensic techniques, but they do not give effective on mobile devices.

In this paper, we remind the classification of the Anti-forensics techniques that have been proposed in arriving at an anti-forensics consensus. Later on we have followed some possible instances of such techniques to the mobile environment and specially to android mobile devices. The instances we followed were fully automated and supported by a common android application called AFDroid.

REFERENCES

[1]. Android debug bridge tool [online]. Available: http//developer.android.com/guide/developing/tools/adb.html.

[2]. Android security architecture [online]. Available:http//developer.android.com/guide/topics/security/security.html;2010

[3]. Android software developing kit [online]. Available: http//developer.android.com/guide/index.html.

[4]. The rise of anti-forensics [online]. Available: http//www.csoonline.com/article/221208/The_Rise_of_Anti_Forensics; 2007.

[5]. Hoog A. Android forensics [online]. Available: http//www.mobileforensicsworld.org/2009.

[6]. Me G. and Rossi M. “Internal forensics acquisition for mobile equipments,” 4th International Workshop on Security in Systems and Networks, proceedings of the International Parallel and Distributed Processing Symposium, 2008.

Author’ biography

Ahmad Talha Siddiqui received his Master Degree M.Tech (CS) from Jamia Hamdard University. Currently he is a Ph.D student at IFTM University, Moradabad. His research interest is mobile computing. He is publishing several papers at international and national journal including IEEE. He is attending IEEE workshop organized by IIT Kanpur.

Shoeb Ahad Siddiqui received his Master Degree M.Tech (CS) from Jamia Hamdard University. He is a Research Schloar student . He is publishing several papers at international and national journal.He is attending IEEE workshop organized by IIT Kanpur.

Mohammad Ibrahim received his Master Degree M.Tech (CS) from Al-Falah School of Engineering and Technology . He is publishing several papers at international and national journal.