Implementation Of Android App With Security Measures

Pradeep Singh

School Of engineering and Science, Lovely Professional University 2, G.T. Road, Near Chehru Railway Bridge, Phagwara (Punjab)-144401, India

Anu Garg

School Of engineering and Science, Lovely Professional University 2, G.T. Road, Near Chehru Railway Bridge, Phagwara (Punjab)-144401, India

Abstract

Android is an operating system for the smart phones and tablets which is based on the Linux. Android was initially developed by Android Inc. and later on purchased by Google and Open Handset Alliance. Android is an open source operating system so the we have to make this operating system very much secure. To provide the security to the assets of our mobile phone like phone book, SMS, confidential files some research works are already done. But this research paper is all about making more security to our mobile phone assets. In this paper, we will see that how to encrypt data or file which will provide the more security to our phonebook and other confidential files. The implementation of this research paper is divided into modules encryption of phonebook, encryption of text file etc. the algorithm which is going to be used in the paper will be Blowfish etc..

General Terms
Security, Algorithms ,Android, Contact

Keywords
Encryption, Contact, Android

1. INTRODUCTION

Android is based on the Linux v2.6 Kernel And is the complete OS ecosystem. While initially it was meant to be a low-cost OS for smart phones and flip-phone devices, it has grown into a mobile OS juggernaut that has practically gobbled up a huge market share. Android offers rich functional support and a full range of computing services which allow devices that run on Android to do much more than stripped down-versions of mobile operating systems. This Operating system not only works for the Mobile Phones but also for some of the home appliances also.

1.1 Open Handset Alliance: Open Handset Alliance is also known as OHA this is the group of the 84 firms who basically develops the open standards for the mobile phones. The firms which are there in the OHA are Samsung, Dell, HTC, Motorola, Intel etc. The OHA was established on 6 November 2007, led by Google with 34 members including mobile handset makers, application developers, some mobile carriers and chip makers

As we are now a days very familiar to the Android Phones so we must know that what are the basic functions which the Android Operating system provides like, how the Android makes a call, how it sends the text messages, and the main thing is that how the setting of the system is being changed and at last that the application which want to use how that apps are installed on the system and how those apps will be uninstalled from the system.

2. SECURITY

It's very important to protect out data from unauthorized user and its not to protect our data but it's very difficult also to protect our data from unauthorized user. So that the person who is not authorized to even see my own data can't make any kid of changes in my data. Following are the terms which are used in security:

Original text: this is the text which is to be sent to the other party.

Cipher text: this is encrypted text which is actually sent to the other party.

There are following two kinds of attacks which a person can do on my data.

Passive attack: the main emphasis of this attack is that the person or we can say that the user who is not authorized can't read my data. Because there can be some kind of important information which should not be read by those person.

Active Attack: active attacks are those kind of attacks which are done on the file or the data in the form of the modification. Or in other words what we can say is that in these kid of attacks the unauthorized user can read the data as well as he/ she can modify the data.

Security mechanism: if we really want to secure our data from the unauthorized user so what we can do is that, we can implement the security mechanism in this we can implement the encryption algorithm, digital signatures and the authentication protocols. By using these things we can make our data secure from the unauthorized user or the attacker who wants to read our data or who want to make some kind of modification in our data.

3. SECURITY ENVIRONMENT OF SMART PHONE

Now a days smart phone can be connected to various subjects like internet, PC, other mobile devices using wireless network. This is the one of the best feature which makes smart phone useful and most popular mobile device.

However, in other words, when we connect the device to the internet then at that point of time malicious attacker or software can invade smart phone in various paths. The Personal Computer can be connected to smart phone by cable or wireless network when we talk about the wireless connection then we can connect our device with Bluetooth or Wi-Fi or any other wireless media, and user may download files or update firmware through PC.

3.1 Smartphone's Assets:

When we are talking about the security of the smart phones then we must know that what are the various assets of the smart phones. because the asset can be regarded by target of attack, and threats and vulnerabilities are basis of the attack.

One researcher has analyzed the types of assets in smart phones (See Figure 1).

Assets	*Description*
Private Information	Address book, Calling history, Location information, Notebook, Schedule, Cache file of web browser, password used in web, email and its attachments, and other information
Device	Smartphone device System resources of smartphone(CPU, RAM, Battery or etc.)
Applications	Smartphone applications user installed

Fig 1: Assets of Smart Phones

4. SCOP OF STUDY

I am going to use some algorithms that will make the encryption more complex so that in any case the phone is lost or stolen and an sophisticated person found that device so that person cant check the data which is there in the device. This app is fully based on the Android so any person who is using the Android smart phone or android Tablet he/she can use this application. In the future this app will help not only for the normal user but also for the army also. As we all know that in the army there are so many things which should be confidential and this app will help them to make the data more confidential . I'll use two encryption algorithm that will make the app more complex fir the hacker. In this app when the actual data is given as an input then the algorithm for encryption will produce a cipher text and that cipher text will be again as an input to other encryption that time it will make another cipher text now finally this cipher text will be saved in the memory. We can see the following scenarios:

Device is stolen/lost and found to a unsophisticated user: if the device is stolen or lost and found to an unsophisticated user. Then he can see all our confidential information or data and he can misuse that data also. In case if we have used the locking system also on our SMS, or important files then also we cant lock out phone book. And at that point of time he can use the brute force technique to crack the password which we have used but if we have encrypted the data and the SMS then at that point of time that user cant access the confidential data.

Device is stolen/lost and found to a sophisticated user: if the device is stolen or lost and found to a sophisticated user then that user can easily crack the password if we have used the password to protect out data and the files. But if we are using the encryption for the security for our data and the SMS then that sophisticated user cant get the original file.

Device is fallen in water or broken: it is the very common thing such that our device is fallen in water or there is any kind of problem due to which we have to face such a problem that we cant access our own smart phone in this condition what we have to do is that, we can use this app .

• **Changing the device**: now a days its very common that we use the smart phone for maximum of 1year because the technology is improving day by day so we have to switch to other phone . incase if we are having a large amount of data which is in encrypted form then at that point of time we have to transfer our data to the computer or any other portable device but if we put all our data into the cloud and then we can easily format our system because formatting the data is more faster as compared to transferring the data, in some cases its also possible that we don't have enough time to transfer the data or we don't have even the device in which we'll save our data then we'll format our device and make an

encrypted backup into the cloud and when we have new Android smart phone or device we can get the recovery.

The objective of this research paper is to make such an app for the android which must be capable to encrypt the text files , our SMS and our phone book as well. I have following objectives for this paper:

• Suppose that we are having some very important contacts in our phone book and we don't want that any other person can check that contact. Then for this also we can use the encryption that will make our data more secure such that if any one want to access the contacts list then he can see only the encrypted contacted and when ever we want to use the contact then we can use software where we can see all the decrypt contacts.

• Secured data transfer with less time is very difficult to achieve. So for this problem this app will give the solution. When ever we insert a memory card this app will scan the memory card and give the list of all the text file and will ask weather we want to encrypt those files or not. If we want to encrypt those file and save it on device then we can.

5. CONCLUSION

In present, there are many researches on Smartphone security, but there is lack of effort to analyze all security threats of Smartphone. To establish Smartphone security, security threats based on Smartphone environment is necessary. Therefore, in this work, we analyzed security of Smartphone and described applicable security mechanisms against threats.

6. FUTURE WORK

As mentioned in the above paper there are some issues in this system related to security. In this paper, I am trying to improve security in an android application like Contacts . in the market also there are some apps which put some passwords on the contacts but those passwords can also be hacked, so I am using some encryption technique so that no one can check out my contacts. We can improve the encryption technique in the future with some latest encryption algorithms

7. REFRENCES

[1]. Jeon Woongryul and Kim Jeeyeon "A Practical Analysis of Smartphone Security" of Information and Communication Engineering, Sungkyunkwan University,

[2]. Enck William "Defending Users Against Smartphone Apps: Techniques and Future Directions" North Carolina State University

[3]. Speckmann Benjamin "Privacy and Security Enhancements for Android Applications" (2008) B.S. (University of Idaho).