User Usage Attack and Security Measure

Jaspreet Kaur

Department of Computer Sciences
and Engineering.
Lovely Professional University
Phagwara

Anu Garg

Asst. Professor at Lovely
Professional University Phagwara

ABSTRACT

Android is an open platform which is becoming very popular operating system. Its open source code is easily handled by the users to get and use new contents and applications on their handsets. Android is totally a permission based process to develop the applications. With the increasing popularity of these smart phones, additional privacy protection to these devices is required. Android is more flexible to become attractive targets for malicious attacks due to significant advances in both hardware and operating systems. Likewise, by installing malicious contents on the device, users can be breached of their security through the compromised information. By compromising user's privacy, malicious applications can access voice recording devices, cameras, intercept SMS messages, usage information or gain location information. Thus the security and privacy are the two most important concerns in android. The need to maintain security and data confidentiality on the Android platform makes it an urgent issue to find loop holes in security.

In this thesis I present an attack on user's usage. This attack allows adversaries to steal the user's usage information and enables attack to get information like what all applications are installed on the mobile, time stamp and date stamp of usage with implementation and a security measure for this spy attack theoretically.

General Terms

Attack, Information, Permissions.

Keywords

User usage attack.

1. INTRODUCTION

At the core, Android security model is a permission-based system that by default denies access to features or functionality that could negatively impact the user experience, the system, or other applications installed on the device [2]. Examples of these features are sending messages or making phone calls, which may incur monetary cost to the user; keeping the device screen on or accessing the vibrator, which could result in battery drain; and reading the user's address book which could result in privacy violations. To make use of the restricted functionality, Android requires application developers to declare which of the restricted features are intended to be used by their application. There are currently 110 items of functionality which are identified as requiring an explicit permission in order for Android to grant access [2].

These permissions control access to network and GPS functions, personal information, system hardware, settings and many other device features. At application install time,

permissions requested by the application are granted to it by the package installer, based on checks against the signatures of the applications declaring those permissions and interaction with the user. No checks with the user are done while an application is running: it either was granted a particular permission when installed, and can use that feature as desired, or the permission was not granted and any attempt to use the feature will fail without prompting the user [2]. The permissions requested by the application and the permissions required to access the application's interfaces/data are defined in its manifest file. Permissions assigned to the user is present with a screen listing that the permissions an application request at install time, to accept or reject which indirectly influence the security policy for the phone. This paper describes how by granting permissions requested by the application can lead to user's usage attack. The permissions requested by the application are not always required by the application for its working. Table 1 shows the analysis done on applications in Android Market that are having wanted and unwanted permissions requesting. As we know Android users are general user and they don't know the meaning and purpose of permissions requested by application. They only know about their requirements that they want this or that application. They will never check whether this permission requested is required by the application or not. In this paper after analyzing the results we came to know how by granting a permission requested by the application, it can lead to information leakage on attacker's side. The information is, what all applications are installed on the mobile, what is the date stamp and time stamp of its usage by the user, which can further give a usage pattern of the user to attacker. The usage generated by the probability that a user will spend a certain time in each operational state for each mode [3]. For example if a person uses facebook at 8:00pm on Monday, 8:00pm on Tuesday, 8:00pm on Wednesday and so on. The attacker will come to know about the usage pattern of the user and shall do another attack to hack user's credentials of a particular application over the network at that time only. This will decrease attackers monitoring time for the data over the network. As Android is becoming popular day by day it is possible that different banks like ICIC, BANK OF BARODA, PUNJAB NATIONAL BANK ETC launch their Android applications to access user's accounts from Android phones directly and threat of stealing credentials will increase.

	Number of applications	Percent
Extra permission(s)	76,366	54.01%
Lacks permission(s)	70,618	49.95%
Exact permission(s)	28,199	19.95%
Reflective method invocation	67,958	48.07%
ClassLoader usage	15,580	11.02%
Total	141,372	100%

Table1: Absolute Number and Properties for Characteristics and Behavior of Android Applications [1]

2. RELATED WORK

In many papers it has been analyzed that the Android developers are requesting for unwanted permissions that the application does not require this in turn provides more access to the developer about the personal information of the user. The attackers are also taking unwanted advantage of the Android permissions to exploit users by developing malicious applications.

3. USER'S USAGE ATTACK MODEL

The usage attack starts when the application is installed by the user. The application at the back end start collecting information of the installed applications in the mobile after that the date stamp and time stamp that is when the user is using that application. All this collected information is stored in database. Then after every five minutes the timer expires and the data is delivered to remote server. The data delivered to the server by an e-mail having the information hacked from the users mobile.

Figure 1: flow chart of user's usage attack

4. USER'S USAGE ATTACK IMPLEMENTATION

It has 4 main modules:

1. Service running in the back ground collects the currently running applications.
2. Collecting the data stamp usage.
3. Collecting the time stamp usage.
4. Sending the collected data to the remote server from the database.

5. SNAPSHOTS OF RESULTS

Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:20:34
Application Name:- WORDS Date Stamp:- 10-04-2013 Time Stamp:- 03:24:07
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:24:15
Application Name:- Facebook Date Stamp:- 10-04-2013 Time Stamp:- 03:24:21
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:24:38
Application Name:- Album Date Stamp:- 10-04-2013 Time Stamp:- 03:24:40
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:24:53
Application Name:- Google Play Store Date Stamp:- 10-04-2013 Time Stamp:- 03:24:56
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:25:04
Application Name:- Gmail Date Stamp:- 10-04-2013 Time Stamp:- 03:25:07
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:26:01
Application Name:- SuperSpy Date Stamp:- 10-04-2013 Time Stamp:- 03:26:12
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:26:12
Application Name:- WhatsApp Date Stamp:- 10-04-2013 Time Stamp:- 03:26:21
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:26:30
Application Name:- Xperia? Home Date Stamp:- 10-04-2013 Time Stamp:- 03:26:38
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:26:43
Application Name:- Xperia? Home Date Stamp:- 10-04-2013 Time Stamp:- 03:27:12
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:27:16
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:28:39
Application Name:- Keypad Date Stamp:- 10-04-2013 Time Stamp:- 03:28:50
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:29:04
Application Name:- Xperia? Home Date Stamp:- 10-04-2013 Time Stamp:- 03:29:24
Application Name:- Facebook Date Stamp:- 10-04-2013 Time Stamp:- 03:29:30
Application Name:- Xperia? Home Date Stamp:- 10-04-2013 Time Stamp:- 03:29:48
Application Name:- Album Date Stamp:- 10-04-2013 Time Stamp:- 03:29:57
Application Name:- Xperia? Home Date Stamp:- 10-04-2013 Time Stamp:- 03:30:04
Application Name:- WhatsApp Date Stamp:- 10-04-2013 Time Stamp:- 03:30:27
Application Name:- Xperia? Home Date Stamp:- 10-04-2013 Time Stamp:- 03:30:31
Application Name:- Dolphin Browser Date Stamp:- 10-04-2013 Time Stamp:- 03:31:09
Application Name:- SuperSpy Date Stamp:- 10-04-2013 Time Stamp:- 03:31:12
Application Name:- Xperia? Home Date Stamp:- 10-04-2013 Time Stamp:- 03:31:12
Application Name:- Facebook Date Stamp:- 10-04-2013 Time Stamp:- 03:31:34

Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:46:25
Application Name:- Facebook Date Stamp:- 11-04-2013 Time Stamp:- 03:46:27
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:46:28
Application Name:- Album Date Stamp:- 11-04-2013 Time Stamp:- 03:46:41
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:46:53
Application Name:- Maps Date Stamp:- 11-04-2013 Time Stamp:- 03:46:57
Application Name:- Settings Date Stamp:- 11-04-2013 Time Stamp:- 03:47:00
Application Name:- Maps Date Stamp:- 11-04-2013 Time Stamp:- 03:47:02
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:04
Application Name:- YouTube Date Stamp:- 11-04-2013 Time Stamp:- 03:47:07
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:13
Application Name:- Google+ Date Stamp:- 11-04-2013 Time Stamp:- 03:47:16
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:23
Application Name:- WhatsApp Date Stamp:- 11-04-2013 Time Stamp:- 03:47:29
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:36
Application Name:- SuperSpy Date Stamp:- 11-04-2013 Time Stamp:- 03:47:43
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:43
Application Name:- Dolphin Browser Date Stamp:- 11-04-2013 Time Stamp:- 03:47:51
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:51:56
Application Name:- Settings Date Stamp:- 11-04-2013 Time Stamp:- 03:52:00
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:52:28
Application Name:- Messaging Date Stamp:- 11-04-2013 Time Stamp:- 06:02:02
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 06:02:23
Application Name:- Keypad Date Stamp:- 11-04-2013 Time Stamp:- 06:11:56
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 06:12:34
Application Name:- Keypad Date Stamp:- 11-04-2013 Time Stamp:- 07:20:57
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 07:21:34
Application Name:- Contacts Date Stamp:- 11-04-2013 Time Stamp:- 08:50:42
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 08:51:11
Application Name:- Messaging Date Stamp:- 12-04-2013 Time Stamp:- 08:45:56
Application Name:- Xperia? Home Date Stamp:- 12-04-2013 Time Stamp:- 08:46:02
Application Name:- Contacts Date Stamp:- 12-04-2013 Time Stamp:- 08:46:03

Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:46:25
Application Name:- Facebook Date Stamp:- 11-04-2013 Time Stamp:- 03:46:27
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:46:30
Application Name:- Album Date Stamp:- 11-04-2013 Time Stamp:- 03:46:41
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:46:53
Application Name:- Maps Date Stamp:- 11-04-2013 Time Stamp:- 03:46:57
Application Name:- Settings Date Stamp:- 11-04-2013 Time Stamp:- 03:47:00
Application Name:- Maps Date Stamp:- 11-04-2013 Time Stamp:- 03:47:02
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:04
Application Name:- YouTube Date Stamp:- 11-04-2013 Time Stamp:- 03:47:07
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:13
Application Name:- Google+ Date Stamp:- 11-04-2013 Time Stamp:- 03:47:16
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:23
Application Name:- WhatsApp Date Stamp:- 11-04-2013 Time Stamp:- 03:47:29
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:36
Application Name:- SuperSpy Date Stamp:- 11-04-2013 Time Stamp:- 03:47:43
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:47:43
Application Name:- Dolphin Browser Date Stamp:- 11-04-2013 Time Stamp:- 03:47:51
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:51:56
Application Name:- Settings Date Stamp:- 11-04-2013 Time Stamp:- 03:52:00
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 03:52:28
Application Name:- Messaging Date Stamp:- 11-04-2013 Time Stamp:- 06:02:02
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 06:02:23
Application Name:- Keypad Date Stamp:- 11-04-2013 Time Stamp:- 06:11:56
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 06:12:34
Application Name:- Keypad Date Stamp:- 11-04-2013 Time Stamp:- 07:20:57
Application Name:- Xperia? Home Date Stamp:- 11-04-2013 Time Stamp:- 07:21:34
Application Name:- Contacts Date Stamp:- 11-04-2013 Time Stamp:- 08:50:42
Application Name:- Messaging Date Stamp:- 11-04-2013 Time Stamp:- 08:51:11
Application Name:- Messaging Date Stamp:- 12-04-2013 Time Stamp:- 08:45:56
Application Name:- Xperia? Home Date Stamp:- 12-04-2013 Time Stamp:- 08:46:02
Application Name:- Contacts Date Stamp:- 12-04-2013 Time Stamp:- 08:46:03

6. CONCLUSION

The conclusion drawn from the above results is that the application requesting for a less priority permissions like System tools retrieve running apps etc can be dangerous as the hacker can draw usage pattern and then can attack for the credentials over the network at that particular hour of the day. As hacker will know that the user uses this application at this time on this day. This attack will decrease the monitoring time of the hacker for credentials over the network. The frequency and probability to get the credentials will increase; hence more credentials can be hacked. So in end we conclude that showing user the permissions requested by the application is not a satisfactory way to increase security as this totally depend on the developer that what all permissions should be requested. User can not change the permissions of the application at installation time. The developers should be fastened or a check should be kept in the development environment that only required permissions are granted. They cannot ask for more permission if the app does not require them.

7. SECURITY MEASURES

1. We can make such inbuilt services with which we can change the names of the applications present on our mobile. If the names are user defined then hacker can never come to know about the installed application on the mobile.
2. In the above attack the update to the attacker is delivered after every five minutes, so we can make a service to monitor the data exchange of an application over the network. The service can then prompt a message to the user that this particular application is doing this much of data ex-change and declare it dangerous.

8. LIMITATIONS:

1. This attack is not able to distinguish between different users.
2. If the time of mobile whose usage pattern we are getting is not the current date and time. That can lead to wrong usage information.

9. ACKNOWLEDGMENTS

The satisfaction that is accomplished on the successful completion of the task would be incomplete without the

mention of the people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I am grateful to Assistant Prof **.Ms. Anu Garg** Computer Science & Engineering Department, Lovely Professional University for the inspiration and the constructive suggestions that helped me to carry out the process of research in this field. Key improvements in the proposed research work would not be possible without the valuable suggestion and the feedback of my guide.

I would also like to thanks to all my colleagues and classmates for their co-operation and support.

10. REFERENCES

- [1] **Analysis of Android Applications' Permissions** Ryan Johnson, Zhaohui Wang Center for Secure Information Systems George Mason University 4400 University Dr, Fairfax, Virginia 22030 Email: {rjohnso8, zwange}/@gmu.edu
Corey Gagnon Department of Computer Science James Madison University Harrisonburg, Virginia 22807 Email: gagnonca@dukes.jmu.edu Angelos Stavrou Center for Secure Information Systems George Mason University 4400 University Dr, Fairfax, Virginia 22030 Email: astravrou@gmu.edu
- [2] **"A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android"**. David Barrera, H. Güneş Kayacık, P.C. van Oorschot and Anil Somayaji. 2010, Vol. Copyright.
- [3] **Personalized Battery Lifetime Prediction for Mobile Devices based on Usage Patterns** Joon-Myung Kang*Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada joonmyung.kang@utoronto.ca ,Sin-seok Seo Department of Computer Science and Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Korea sesise@postech.ac.kr ,James Won-Ki Hong
Division of IT Convergence and Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Korea
jwkhong@postech.ac.kr Journal of Computing Science and Engineering, Vol. 5, No. 4, December 2011, pp. 338-345