ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

TECHNICLE NOTE

Available Online at www.ijarcs.info

Android Mobile Security – An Issue of Future

Dr. S. O. Khanna*
Professor, MSc (IT) Department
Institute of Science and Technology for Advanced studies and Research (ISTAR), V.V.Nagar, Gujarat(India)
sonukhanna@yahoo.com

Mr. Pritesh Patel
Assistant Professor, MCA Department
Institute of Science and Technology for Advanced studies and Research (ISTAR), V.V.Nagar, Gujarat(India)
patelpritesh2484@gmail.com

Abstract - Now a day's a mobile became a part of life. Mobile phone had changed the life style of the human being. People uses mobile for communication, internet surfing and for business. Due to the large community of users there are various companies introducing new mobile phones having novice functionalities. But there may be a security threats from intruder like hackers. This paper presents various security flaw of android mobile which is a serious matter of futures as android technology booms the market of mobile phones. This paper also presents some security measures to put android mobile phone away from hacker and viruses.

Keywords: Android, Hacker, Delvik, Geinimi, Security Flaw

I. INTRODUCTION

Today trend is for small mobile devices and high processing power. A few years ago, the choice was between a wireless mobile phone and a simple PDA [9]. Smartphone a new category of mobile phone combine the best aspects of mobile and wireless technology creates new business tools for user. Different companies design various smartphone for unique purpose. Android smartphone mobile phone becomes popular and as the Android world grows, it becomes an increasingly juicy target for malware. Infected apps have been spotted in various Android app outlets on numerous occasions. The platform is less restricted than Apple's, for example, and with those freedoms sometimes come security dangers. Critics say Google could address Android's security issues with a few tighter control policies. The number of attacks on Android devices has been rising over the past few months.

II. INTRODUCTION TO ANDROID

Android is an operating system (OS) developed by Open Handset Alliance (OHA). Android is also known as a software stack for mobile devices that includes an operating system, middleware and key applications. The Alliance is a coalition of more than 50 mobile technology companies ranging from handset manufacturer and service provider to semiconductor manufacturers and software developers, including Acer, ARM, Google, eBay, HTC, Intel, LG Electronics, Qualcomm, Sprint and T-Mobile [8]. The stated goal of the OHA is to "accelerate innovation in mobile and offer consumer a richer, less expensive, and better mobile experience". By providing an open development platform, Android offers developers the ability to build extremely rich and innovative applications. Developers are free to take advantage of the device hardware, access location information, run background services, set alarms, add notifications to the status bar, etc.(*developer.android.com, 2011).*

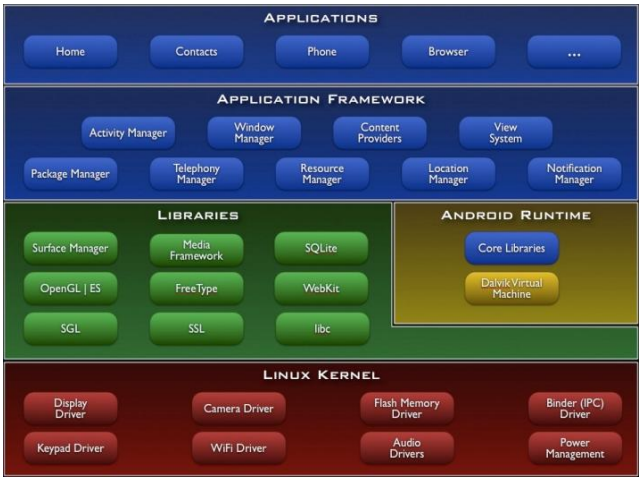

Figure. 1 Android Architecture (developer.android.com, 2011)

Basic architecture of android is shown in fig. 1. Android OS is built on the Linux 2.6 kernel. The Android Runtime System utilizes Delvik virtual machine (VM), which allows multiple applications to be run concurrently as each application is its own separate VM [8]. Android application compiled into Delvik executable (.dex) and is run by Delvik virtual machine. Android provides a substantial set of abstractions for developers, including ones for user interfaces, application life cycle, various application types, efficient IPC mechanisms, and permissions [12].

Android is a privilege-separated operating system, in which each application runs with a distinct system identity (Linux user ID and group ID) and parts of the system are also separated into distinct identities *(developer.android.com, 2011).*

III. ATTACKS ON ANDROID

Android is considered as successful software stack consisting of an operating system, middleware and some key applications bundled [10]. Android has the enough potential to become the dominant OS for smartphones around the globe. The problem lies in Android's security architecture, and the proof is that it's easy to build applications that can get access to sensitive operating system resources such as

text messages, voice and location [1] based services. Google doesn't check apps before letting their author's post them on the Android Market [1] so there are chances of uploading fake or malicious application that can harm to the user.The malware has exotic names such as "Zitmo," "DroidDreamLight," "Hong Tou Tou," "DroidKungFu," "YZHCSMS," "Geinimi" and "Plankton [1].

In china the malicious application named "Geinimi," gains access to personal information of the users and sends the location and other details including IMEI number and SIM card information, to a remote server after every five minutes and is found to communicate with a central command-and-control server and the hackers can command the phone to download and install other programmes [2]. Sometime warnings appear for the most innocuous things, which leads to users quickly tapping OK, even when something shows up that shouldn't, like the ability to record your calls and send them to a third party. You can see a collection of permissions which apps can potentially show users. You'll notice that the permissions list is quite long, and when you look at an app on your device the list requires a decent amount of scrolling [5]. The researchers wrote in a blog that those people, using Android devices running versions 2.3.3 and below, might come under attack, when they are connected to unencrypted Wi-Fi networks [3].

DroidDream and GGtracker were stated to be most infectious malware [4]. The makers of DroidDream made 80 different versions of the app creating trust in the users whereas GGtracker signed up users for premium services without their consent and users were charged from $10 to $50 for signups [4]. GGracker also mal advertising in which advertisements prompted users to visit malicious websites which intern automatically download malware to the device, when visited [4].

IV. PRECAUTION MEASURE FOR SAFETY

Various precautions must be taken to prevent or put away the intruders and viruses from android smartphone. These precautions must be taken by user of android mobile phone and application developer. Google is relying on third party vendors like Lookout to handle security. Third Parties can do a good job of protecting users, but a large number of Android users don't even know about the built-in security functions let alone to go out and look for malware protection [5]. It's important to note that the "auto-answering" feature of the malware can only affect phones running Android versions 2.2 and below, as the MODIFY_PHONE_STATE permission was disabled in Android 2.3 [6]. The users of android mobile should only download apps from trusted websites and be more cautious about unexpected phone behavior such as slowing speed and phone reboot [4].

Implement strong asset management, virus checking, loss prevention and other controls for mobile system that will prohibit unauthorized access and the entry of corrupted data [9]. Remove the applications downloaded from Driod09. To protect the android phone from phishing lookout mobile security in new browsing features and don't click on suspicious web links. Store your password and data in an encryptions application. Install latest anti-virus software and firewall software to detect and stop any infections and intrusions. If your application accesses or uses private data, especially usernames, passwords, or contact information, it's a good idea to include an End User License Agreement (EULA) and a Privacy Policy with your application [11]. Never expose data in content provider without providing appropriate permission in application and never work around any security mechanism provided by android framework. Remember to use encryption classes for securing sensitive data provided by android framework.

Make sure any servers or services that your application relies upon are properly secured against identity or data theft and invasion of privacy [11]. Along with this google is trying to fix the security holes in its future versions. Prevent SQL injection via parameterized queries that distinguish data from query logic explicitly. The ContentProvider's query(), update(), and delete() methods and Activity's managedQuery() method supports parameterization [12] and provides clear separation between the content of the SQL statement in the "selection" parameter and the data being included and prevent confusing the database and SQL Injection is avoided.

V. FUTURE WORK

As android market is vast and having large number of users. New version of android framework and phones may be come in market. So in future we will try to find more flaws in android and try to find and provide solution to prevent the attack.

VI. CONCLUSION

It is concluded that android mobile phone user must take some precaution measure to put away the intruder and viruses. Different types of security measure software, encryption software and ant-viruses software must be used. User can also design own custom software to prevent the attack. Attack can also be prevented by having detail knowledge of mobile phone and its behavioral architecture. Developer can design application by implementing some security measure, inbuilt security classes to design and develop application.

VII. REFERENCES

[1]. http://www.technewsworld.com/story/73036.html, Retrieved 18th, Aug, 2011

[2]. http://newstonight.net/content/security-experts-detect-trojan-targeting-android-devices-china, Retrieved 18th, Aug, 2011

[3]. http://www.ibtimes.com/articles/197761/20110815/expert-claims-android-os-has-serious-security-flaws-goolge-declines-operating-system-mobile-security.htm, Retrieved 19th, Aug, 2011

[4]. http://newstonight.net/content/malware-infections-increase-twice-android-devices, Retrieved 18th, Aug, 2011

[5]. http://www.gottabemobile.com/2011/08/04/security-is-android-the-windows-xp-of-mobile, Retrieved 19th, Aug, 2011

[6]. http://techcrunch.com/2011/08/15/new-android-malware-hides-as-google-app-answers-calls-for-you/, Retrieved 23rd, Aug, 2011

[7]. Android Forensics: Investigation, Analysis and Mobile Security for Google Android (Syngress) By Andrew Hoog

[8]. Android Forensics: Simplifying Cell Phone Examination By Jeff Lessard and Gary C. Kessler, Small Scale Digital Device Forensics Journal Vol. 4, Issue. 1 Sep 2010, ISSN: 1941-6164

[9]. Cyber Security – Understanding cyber crimes, computer forensics and legal perspectives, By Nina Godbole and Sunita Belapure, Wiley India ISBN 978-81-265-2179-1

[10]. CSI Communication – Mobile Application Development, ISSN 0970-647X, Vol. 35 Issue. 1 April, 2011 pg. no. 11

[11]. Android™ Wireless Application Development, 2nd Edition, By Shane Conder and Lauren Darcey, Pearson Education, Inc, ISBN 978-0-321-74301-5

[12]. Mobile Application Security By: Himanshu Dwivedi, Chris Clark and David Thiel, McGraw-Hill, ISBN 978-0-07-163356-7