A Critical Evaluation of Vulnerabilities in Android OS: (Forensic Approach)

Buthaina Mohammed AL-Zadjali
Sohar University, Computing Department
Sohar, University Rd, 311
Sultanate of Oman

ABSTRACT
The Android platform is an open source operating system, which is widely used on Smartphones. Android operating system usage and adaptation is rapidly increasing with a variety of applications. It also, allows developers to freely access and modifies source code. The open nature of the Android platform attracts attackers to do different types of criminal activities. The android users likely to install and download many applications which can be contain malicious code written by software hackers. The purpose of this paper is to explore the most significant security threats and vulnerabilities in the Android Operating System.

General Terms
Android OS, Vulnerabilities, Linux Kernel.

Keywords
Android Smartphone, Vulnerabilities, Security threats, Android Architecture.

1. INTRODUCTION
Android is an Open Source platform and it is fast growing and the largest installed base of Mobile platform, which empowers many mobile devices. It is based on the Linux kernel, and it is developed by Google and the Open Handset Alliance. The most features of this platform, it allows developers to write managed code in a Java language, but does not support programs developed in another code. The unveiling of this platform was on 5 November 2007 with the founding of the Open Handset Alliance and it was released in 2008.

In addition, it is flexible to run on different mobile devices having various hardware configurations. This mainly increases the popularity and acceptance of android amongst most of the users (Nimodia & Deshmukh 2012) . Nowadays, Smartphones becomes as a very useful device in people pocket but the attacker exploit this technology as a tool for criminal activities. The newer features of these Smartphone like location awareness, GPS, Bluetooth and Wi-Fi hacking become the easiest way for attackers to launch sophisticated criminal activities.

2. ANDROID PLATFORM
The Android platform is the most popular Operating system with various types and versions. The most features of Android is the open source platform and this feature not only establish a new direction for the industry but also, it opens the door in front of developers' code savvy forensic analysts and the criminals understand the device at the most fundamental level. The Android is the core platform which quickly matures and provided free of charge for carriers and hardware vendors. In addition, it is focusing their efforts in all customizations to retain their customers (Hoog 2011) .

According to the last statistic of which focus on the smartphone in the Market the Android got a 80.2 % share of all users globally in 2014, while the other types got less than Android and this result gives us a full picture of Android Smartphones are the most popular platform in recent years. The following chart illustrates the results of the Global Smartphone in the Market (Edwards 2014).

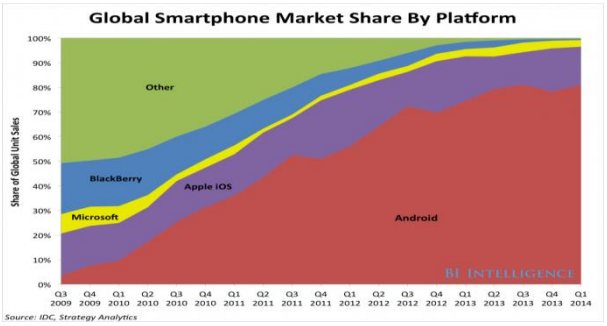

Fig 1: Android Smartphone in Global Market

2.1 Android Versions History
The development process of Android platform update rapidly and the new versions of this platform released with new features and bug fixes. However, table 1; illustrate the detailed information about the Android History version (Kumar & Haq 2011).

Table 1: Android Versions History

Version	Name	Linux Kernel Version	Release Date
1.0	Alpha	-	23/09/ 2008
1.1	Beta	-	09/02/2009
1.5	Cupcake	2.6.27	30/04/ 2009
1.6	Donut	2.6.29	15/09/2009
2.0/2.1	Éclair	2.6.29	26/10/ 2009
2.2.x	Froyo	2.6.32	20/05/2010
2.3.x	Gingerbread	2.6.35	06/12/ 2010
3.x	Honeycomb	2.6.36	22/02/ 2011
4.0.x	Ice cream sandwich	3.0.1	19/10/2011
4.1/4.2/4.3	Jelly Bean	3.0.31	09/07/2012

4.4	KitKat	3.4	03/09/ 2013
5.0	Key Lime Pie	3.8	10/2013

Based on table 1, the following features of each Android Versions (Kumar & Haq 2011):

- **Alpha and Beta:** the initial release of Android platform.
- **Cupcake:** The main feature of this version is the User Interface (UI) update for all core elements , on-screen soft keyboard, accelerometer-based application rotations , playback , video recording, Bluetooth .
- **Donut:** This version support higher screen resolutions (WVGA), Virtual Private Network & 802.1x and text-to-speech engine.
- **Éclair:** The major UI update, media framework improvement, Bluetooth 2.1 and support the Microsoft Exchange.
- **Froyo:** Performance optimizations, Wi-Fi hotspot capability and tethering, Open GLES 2.0, Adobe Flash support and enhanced Microsoft Exchange support.
- **Gingerbread:** In this version add new features for the User Interface to make it faster and more simple such as text input and Improved power management, Support for Internet/SIP calling (VoIP), One-touch word selection and copy/paste, NFC Reader application lets the ,communication (NFC) tags and Camera improvements.
- **Honeycomb**: Improved and extended support for near-field communications (NFCs), Tweaks to Bluetooth, graphics, media framework, speech recognition and Support for 57 languages/locales.
- **Ice cream sandwich**: The improvement of this version includes a variety of features such as, new lock screen, quick responses of incoming calls, text input improved, spell checking, tasks and browser tabs (Android Developers n.d.).
- **Jelly Bean:** High performance than the previous versions because it is faster and smoother. It consists of OpenGL ES 3.0 for high graphics resolution, enhance the Bluetooth connection and include new Media such as VP8 endcoder Media muxer, playback progress and Modular DRM framework (Android Developers n.d.).
- **KitKat:** New capabilities of NFC through Host Card Emulation, Low-power sensors, Storage, Screen recording, access framework, SMS provider and Printing framework. Common Encryption for DASH, Wi-Fi CERTIFIED Miracast, SELinux (enforcing mode) and GLES2.0 Surface Flinger (Android Developers n.d.).
- Key Lime Pie: The main features of this version is the Google Bable which can Integrate various popular messaging options into one service such as (Talk, Voice, SMS Email and others)(Tom Smith 2013).

2.2 Android Architecture

The Android platform consists five layers and each layer of Architecture provides different services for the other layers. The highest layer in the Android Architecture is the Application layer and the lowest layer is the Linux Kernel. The other layers are, Application Framework, System Libraries, Android Runtime (Shewale et al. 2014).

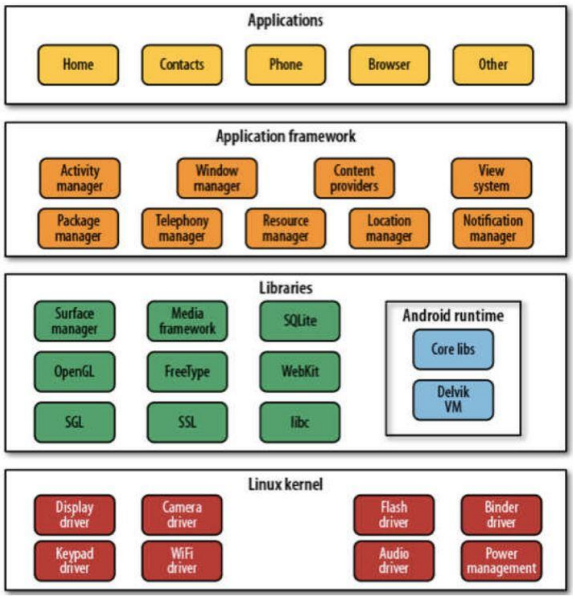

Fig 2: Android Architecture (Marko Gargenta n.d.)

2.2.1 Application

Android comes with the set of basic built in application like E-mails, contacts, calendar, SMS and Web browser which records in top section. The application is generally written in Java language and all run on own process where some application already installed on the Android Smartphone while some are free to download from the internet. It also provide feature API's for building innovation application such as a location manager.

2.2.2 Application Framework

It is a component based framework written in Java. This architecture is designed in such way that provides reusable components which can use the same framework and use APIs, making it simple to write application for example scrollbar elements which use many components. It has some activities that are performs through the graphical user interface. Services component do not contain any user interface /GUI thread. It can declare in the XML file "AndroidManifest.xml".

2.2.3 Libraries

The Android system provides some C/C++ libraries. The component of Android platform it utilize through the libraries media libraries which provides playback & streaming in different standards format & audio, video and image and surface manager for composing different drawing surface onto the screen. SQL lite for the data storage, webkit to the open web browser engine.

2.2.4 Android Runtime

It consist of these things first one libraries and the second is the Davlik Virtual Machine specially designed for the less powers usage and space used by the application in the Android system. It is built mainly to support its embedded environment with limited CPU, battery and small screen. Davlik use highly optimized CPU, data shared to all

applications in such way that there can be multiple instances at a given time.

2.2.5 Linux Kernel

Android is built in the Linux 2.6 GPL v2 licensed with approximately 115 patches. It is the hardware abstraction layer which controls the hardware and it is resources. It provides basic functionality such as memory management, network stacks for communication and control process, network and power management and proven to be very stable.

2.3 File System and Storage Media in Android

2.3.1 File System

From a file system perspective, the Android Operating system used the file system to organize the file in an efficient manner. Android, based on Linux file system and many of the file system used to boot and run the device. The types of the file system on Android are EXT, FAT32 and YAFFS (Yet Another Flash File System) known as the first NAND optimized Linux flash file system and it is used for booting (Vijayan et al. 2012).

2.3.2 Data Storage

The data storage unit is the most important part in all devices and when it comes to configuring and setting up the storage in mobile devices the traditional hard drives are in general too big and consume too much power to be useful. In contrast, the flash memory devices provide fast access and read for data better than the hard drives. There are two types of flash memory devices which are NAND and NOR. The NOR based solution provides lower density and can characterize as slow write and fast read components. NAND based solution offers low cost, high density and are labeled as fast write and slow read. In some embedded system use of NAND flash devices for data storage and NOR for code execution environment (Heger 2012).

Android Smartphone store more data than other standard phone. Furthermore the Android phone can store data in five methods which are internal storage, external storage, SQL lite, the network and the developer that can store key-value pairs of primitive data in an XML format. Android store much of data in external memory like NAND flash memory. SD Cards are used as external storage and loaded with FAT32 file system and this type of file system is not more secure like other file system ext3 and ext4. SQLite is a database format appearing in most of Mobile system. In addition, it is lightweight and it's entire by code base. The SQLite files are stored in the internal storage. The network also can be used to store and retrieve data (Vijayan et al. 2012).

3. ANDROID SECURITY THREATS

The additional hardware in the Android smartphone such as camera, GPS, Wi-Fi and other software make the Linux layer more vulnerable. The security threats which can apply in the modern operating system also can be applied to the Android platform.

There are different types of security threats can affect the Android platform. The network is the most security threat which the attacker exploits to attack users' smart phone. These attacks can exploit the weaknesses come from different types of access, such as SMS, MMS and Wi-Fi network. In addition, there are some modules which also can effect on mobile system, including the Android system such as SMS, Spyware and Malware. The Malware can be classified into more than one type such as, Trojan horse, Botnet, Worms and Rootkit (G. Delac 2011).

The network security threats in the smartphone have higher impact than the desktop computer or server because in the smartphones does not use the static network as the desktop computer and server. All types of smartphone require to connect to the network through the 3G , 4G or Wi-Fi and this thing make it more vulnerable to network attacks such as spoofing or sniffing. The advantage of not assigned the smartphone to any static network give the user flexibility to move to anywhere without any restrictions, but that can reduce the security layers of protection for the smartphone. There are different types of security threats in Android, as discussed in the following points (Marko Gargenta n.d.):

- **Wi-Fi connection:** Is one type of security threats which can exploit the vulnerability in the Android operating system. The attacker can eavesdrop and access to content of Android without the user permission. There are many good tools which take the advantages of LAN/Wi-Fi and help the attacker to exploit the vulnerability in Android device.

- **Application:** Other security threats is the application which is downloaded from the Android Google play, may contain some malicious code which can exploit the Android platform. The developer can deploy an application and some of these applications contain different types of Malware and installing these applications will affect the operating system.

- **Camera and GPS:** The running software's and drivers generally secure by default. Main issue lying are lack of privacy due to the hacking software tools open market, which can be used to track the device and also the photos taken from the same can be misused or in other words steal.

- **Bluetooth:** Is essential to connect the external devices such as headphones, but it can be vulnerable as it is used to control the device and misuse the confidential or secret data's.

3.1 Android Security Mechanisms

Some of the features in the Linux kernel are the user identifier and prior multitasking which enforces the security between file system and applications. On the desktop Linux is opposite than Android where all applications can execute by user with the same user id. In Android operating system each application assigned with a unique identifier and a separate instance running on the virtual machine shares its own code that runs memory and process.

The permissions for installing any application in the Android system based on mechanism to enforce security restrictions and this restriction depend on user to allow or deny installing the applications. By default, the Android system didn't allow installing any application from unknown sources, but the user can change the permission of access to unknown resources. In addition, Android used other security mechanisms known as sand-boxing to implement the multiprocessing of application (Kumar & Haq 2011) .

4. VULNERABILITY ANALYSIS IN ANDROID

Vulnerabilities in Android are frequently evaluating because the Android devices are relatively new in the market.

Moreover, the releases of new models of the Android operating system have constantly been the main concern of most security companies because it is not easy to identify the security risks in this platform. For that reason, the Android platform is widely targeted and susceptible to exploit by attackers (Jovanovic 2012). In addition, to discover the vulnerabilities in Android system, it should conduct penetration testing to examine the weakness in the Android Architecture and establish appropriate solutions to reduce the vulnerabilities.

The most related works regarding the security of Android smartphone have focused on the application layer, such as viruses, worms, MMS exploitation and Cross-Service Attacks. The research work on the security of mobile operating system began in 2000 and 2001which focused on security of memory protection and permission based file access control (Kumar & Haq 2011).

4.1 Identifying vulnerability in Android

There are some threats/vulnerabilities on Android devices that might be reason for concern. It covers a significant range of the vulnerability and risks which can exploit the Android Operating System (Juniper 2012).

- Users as admin install apps, download data and access unprotected networks this resulting to use the Android domain without any restrictions.
- The Google verification process lacks during the last 2 years leading to dangerous malware infected apps in the Android Market.
- Any Android phones connected to computer through USB cable easily hacks the contents of the SD-Card to Read/Write/Delete. This will result in bringing malware in corporate network for downloading malicious contents through the gateway of PC.
- While data transfers between virtualized application environments, there is full risk of transmission of malicious application injections resulting data being compromised as a target app respond to the string resulting data loss.
- Rooting is also a common exploit used by malicious applications to gain system level access to Android. Dsploit is one such threat that can root a system, kills connection, makes redirection and escapes detection by penetration to deliver a payload and change the contents of the phone like images.
- A wireless network is vulnerability in Android devices running 2.3.3, which needs to compromise an unprotected Wi-Fi. Ideally, sign in credentials should always be completed over secured network, but sometimes this is not enough. An Android application name FaceNiff released in June 2012 allows hackers to stop the web session profiles over Wi-Fi and steals the user credentials for Facebook, twitter, YouTube and other social media. It generally works in encrypted network. The only way the FaceNiff will not work is to use SSL. Wi-Fi hotspots globally expected to grow more than 5.8 million by 2015 according to Juniper Mobile Threats report 2011.
- With Wi-Fi, hacking there is also MAN-IN-THE-MIDDLE attacks that are widely available online like WIRESHARK application, which enables hackers to intercept the emails of mobile phone users that could contain sensitive and valuable information or data.

Fig 3 and 3.1, displays the statistics of the vulnerability on Android Phones according to Google year 2009 to 2015 (www.cvedetails.com 2015)

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	11	1	4	1		1				1	2	1			
2015	69	22	43	36	17					12	9	1	1		
Total	110	34	55	41	20	1				18	15	8	1		1
% Of All		30.9	50.0	37.3	18.2	0.9	0.0	0.0	0.0	16.4	13.6	7.3	0.9	0.0	

Fig 3: Android Vulnerability Trends over Time

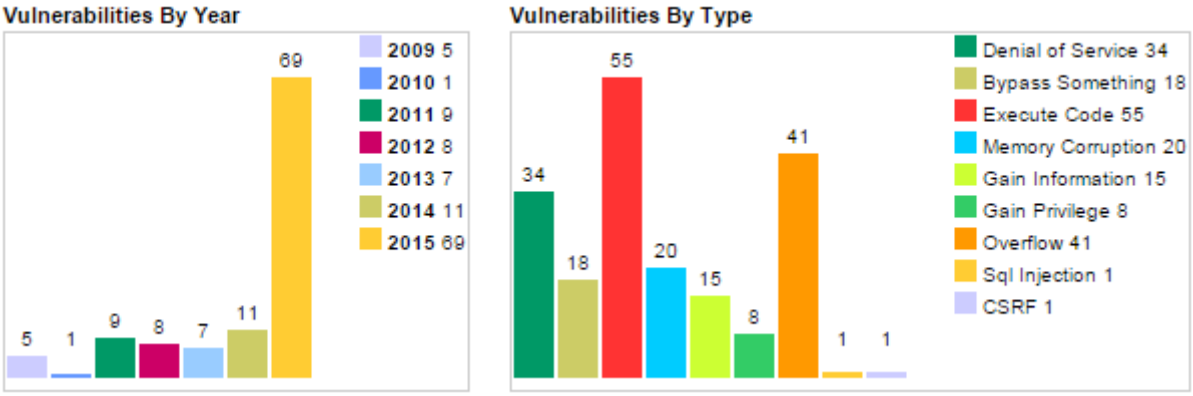

Fig 3.1: Android Vulnerabilities by Years and Types

5. CONCLUSION

After exploring the most significant security threats and vulnerabilities in the Android Operating System, it's clear that these vulnerabilities can impact the Android users. To reduce the number of increasing vulnerabilities, the developers of Android Operating system should introduce new security enforcement and exploit mitigation techniques. The hardware in the Android smartphone such as camera, GPS, Wi-Fi and other software make the Linux layer more vulnerable. To avoid duplicating the same vulnerabilities again in Android Linux Kernel the vulnerability fixes released for these should be mended. The smartphone users should be more aware about their personal data and the permissions granted during installation of any application from official Google play store. Nowadays, the Smartphone's illegal activities have increased and the hacker uses different ways and techniques to access the victim's devices. For that reason, the individual users need some advice to increase their awareness of how to protect their mobile phones from any hacker.

6. FUTURE WORK

After analysis the Android security threats which can affect Android platform, the future work will involve to selecting one type of these threats which is Wireless access point (Wi-Fi) to evaluate the vulnerability in Android by conducting the penetration test through Wi-Fi and to proof if possible to attack the Linux Kernel through it.

7. REFERENCES

[1] Android Developers, Android Developers Jelly Bean.Availableat:http://developer.android.com/about/index.html.

[2] Edwards, J., 2014. Global Smartphone in the Market.Availableat:http://www.businessinsider.com/iphone-v-android-market-share-2014-5.

[3] G. Delac, M.S. and J.K., 2011. Emerging Security Threats for Mobile Platforms,

[4] Heger, D., 2012. Mobile Devices-An Introduction to the Android Operating Environment Design, Architecture, and Performance Implications. DHTechnologies (DHT), retrieved March, pp.1–6. Available at: http://people.stfx.ca/x2011/x2011bhd/391/m_78_3.pdf.

[5] Hoog,A.,2011.AndroidForensics:Investigation,AnalysisandMobileSecurityforGoogleAndroid,Availableat:http://www.elsevier.com/wps/find/bookdescription.cws_home/725477/description#description.

[6] Jovanovic, Z., 2012. Android Forensic Techniques. , p.20.

[7] Juniper, 2012. 2011 Mobile Threats Report. 2011 Mobile Threats Report, (February), pp.1–23.

[8] Kumar, N. & Haq, M., 2011. Penetration Testing of Android-based Smartphones Naresh Kumar. , (June).

[9] Marko Gargenta, n s t i t u t e u t h o r r e t a i n s f u l l r i g h t s First Edit. A. O. and B. Jepson, ed., O'Reilly Media, Inc.

[10] Nimodia, C. & Deshmukh, H., 2012. Android Operating System. Software Engineering, ISSN, 3(1), pp.10–13. Available at: http://www.bioinfo.in/uploadfiles/13366356953_1_1_SE.pdf.

[11] Shewale,H.etal.,2014.Analysisof Android Vulnerabilities and Modern Exploitation Techniques. Ictactjournals.in, 6948(March), pp.863–867. Available at: http://ictactjournals.in/paper/IJCT_Paper_1_863_to_867.pdf.

[12] Tom Smith, 2013. Android 5.0 Key Lime Pie features, release date with Nexus 10 2 and Nexus5[Rumors].Availableat:http://www.christiantoday.com/article/android.5.0.key.lime.pie.features.release.date.nexus.10.2.nexus.5.rumors/33635.htm.

[13] Vijayan, V., Ludwiniak, R. & McCara, G., 2012. AndroidForensicCapabilityandEvaluationofExtractionTools.,(April).Availableat:http://www.academia.edu/1632597/Android_Forensic_Capability_and_Evaluation_of_Extraction_Tools.

[14] www.cvedetails.com,2015.vulnerabilityonAndroidPhones.Availableat:http://www.cvedetails.com/product/19997GoogleAndroid.html?vendor_id=1224.