A comparative scrutiny of smartphone Operating Systems

Abhishek Yadav, Surabhi Maheshwari

BE Student (CSE Dept. Lakshmi Narain College of Technology, Bhopal, India)

ABSTRACT: Nowadays, a variety of mobile phones with different operating systems are available in the market but mobile phones with android OS have now become indigenous product which was once extravagant product. The purpose of this change is credited to its varied functionality, ease of use and utility. There are various tasks executed on it like making call, sending or receiving SMS, music, billing, online shopping, online booking, playing games, and web browsing, with the help of different applications like Whatsapp, Facebook or Applock etc. Thus, a huge quantity of user sensitive data is stored within the devices. With the increased usage of smartphone, the security of user-private data is a big concern. Because of android as an open source mobile platform, third party applications from markets and even from unreliable sources can be easily installed by the user. Thus, Android devices are a easy-going target for privacy intrusion. This paper is a review and examination of android software stack and comparison of smartphone based operating system like android, iOS, blackberry, Symbian, windows phone, webOS, Ubuntu and firefox.

KEYWORDS: Android software architecture; android; iOS; Symbian; blackberry; windows phone; webOS; Ubuntu; Firefox; Android Security

1. INTRODUCTION

Smartphones are now joining almost in each and every domain of life like business, education, workplace and healthcare. The Worldwide Mobile Communications Device Open Operating System Sales (WMDOOS) offers complete market of 104,898 to End Users by OS [3]. There are above 1.3 million active applications [4] in Google Play App Store. Android is the first open source, Linux-based and modern mobile handset platform. Google established it for handset manufacturers like T-Mobile, Sprint Nextel, Google, Intel, Samsung, etc. [1]. It provides to customers a richer, less costly, well mobile experience and numerous attributes like 3D, SQLite, Connectivity, WebKit, Dalvik and FreeType etc. Since

This work is licensed under a Creative Commons Attribution 4.0 International License.
android offers open source operating system; users and developers can acquire source code but only below the rules and conditions [1]. Whenever the user needs to install any application, first of all its description as well as a list of permission requests is provided with an opportunity for review beforehand its installation or cancel the installation if he or she realizes that the permissions are too many or objectionable. The android operating system has its own well developed android permission model, but intruders can supplement them by permitting the components to be altered within and through the applications across Intent communication mechanism due to which it has vulnerability for attacks by malwares [5].

Android open source platform necessitates strong and complex security architecture to guarantee security of user private data, personal information, application and network, but it has little constraints for developers which increases the security threat for the end users [2].

This paper is to contrast the modern smartphone operating system like android, iOS, blackberry, Symbian, windows phone, webOS, Ubuntu and Firefox. The contrast between diverse smartphone operating system is done using various parameters like OS family, Environment and market share. After summing up findings through the comparison, the conclusion discusses which operating systems are in race and produce some deductions from it.

The rest of the paper is organized as follows: section 2 presents the android architecture diagram: software stack of android, section 3 presents the related work, section 4 show the comparison of different major operating system, section 5 includes conclusions and future scope of the research work.

2. SOFTWARE STACK OF ANDROID

Android OS is architected in the arrangement of different layers of stacked as software that includes android applications, an operating system, android run-time, middleware, services and libraries. Each layer of the stack, and the corresponding elements within each layer, are firmly integrated and delivers different kind of services to the layer just above it as well as the optimal application development and execution environment for mobile devices.

The Software stack of android contains of different layers that offer different services to layer just above it are shown in Figure 1.
1. Linux Kernel - heart of whole system
2. Libraries and Android Runtime
3. Application Framework

2.1 **Linux Kernel - the heart of the whole system**

At end of the Software stack of Android, there is a Linux kernel. It behaves as the core of the whole system. It offers various functionalities like memory management, process management, device management, security settings etc. in android system and all the essential device drivers for the hardware with which it cooperates [1].

2.2 **Native Libraries**

On the top of the kernel layer there is a group of libraries including surface manager that comprises windows on the screen, Open GL|ES for 3D Library, SGL for 2D Graphics, Media Framework to play and recording of numerous audio, video and picture formats, Free Type
for Font Rendering, WebKit Browser Engine, well known libc for System C libraries, SQLite relational database for storage, Open SSL internet security library etc. These native libraries are centred upon c or c++ language.

2.3 Android Runtime

Located on the same status as the native libraries, the Android runtime is the third unit of the architecture and accessible on the second layer from the bottom. It contains a group of essential Java libraries that allows Android application developers to write Android applications with the help of standard Java programming language. It also contains ART (Android Runtime) [7]. It is a alike to DVM (Dalvik Virtual Machine) specially designed and optimized for Android. Each procedure is performed in a virtual machine separately. It works on DEX files and running dex byte codes. It offers Ahead-of-Time (AOT) compilation, better garbage collection, enhanced debugging and development, security, isolation, memory management, fast performance and threading support. It supports user to execute numerous applications at the same time.

2.4 Application Framework

On the top of Native libraries and android runtime layer, there is application framework layer. It delivers many packages of higher-level services to application that together form the environment within which they are built from reusable, exchangeable and replaceable constituents. It provides the roles of phone like location management, data sharing, resource management etc.

The packages present are as given below:

2.4.1 Activity manager

It administers and manages the action lifecycle of applications.

2.4.2 Resource manager

It manages and delivers access to non-code embedded resources such as graphics, strings, colour settings and user interface layouts.
2.4.3 Notification manager
It permits all applications to display custom warnings in status bar and notifications to the user.

2.4.4 Location manager
When user arrives or quit a particular geographical location, it triggers alerts about location changes using GPS or cell tower.

2.4.5 Package manager
The system by which applications are able to retrieve the data about other applications currently installed on the device.

2.4.6 Telephony manager
It manages and enables to access voice calls, network connection settings, status and subscriber information service in our application.

2.4.7 Window manager
An extensible set of creative views and layouts is used to create application user interfaces.

2.4.8 Content Provider
It is the system by which it enables and manages data sharing between applications [1].

2.5 Android applications

The android applications are at the topmost protect of the Android software stack. These constitute both the native applications and the third party applications. The native applications laid at one feet the integral Android implementation a well known as SMS easy make app, Dialer, Web user and Contact manager. The third party applications are besides installed individually developers, programmers’ interruption debugging/testing and user after purchasing the device.

3. RELATED WORK
As android practice is increasing constantly, so android have appeared as an exceptional area of investigation in latest past. Research activities are focused in areas such as reverse engineering, clustering, machine learning, operating system and security and they have acknowledged a share of attention. Since the proposed work is focused on operating system and security, this study covers the above two areas with respect to smartphones based operating system.

In 2014, Kaur et. al. [1], described the android architecture, android operating system and its important features. They also contrasted Android with different OS like iOS (Apple), Symbian (Nokia) & Blackberry OS (RIM). From their investigation, they deduced that android is superior than all other operating systems. However, because of open source OS and exclusive characteristics, android has some curbs which leads to malware attacks like virus, worms, spyware, adware and Trojan horse.

In 2014, Dabhi et. al. [7], offered a detail examination on modern and imminent operating systems like IOS 7(Apple), Android 4.4 KitKat (Google) and windows 9 (Microsoft). They paralleled updated features, facilities, performance and decision about these operating systems. From market share analysis during December 2013, They discovered that android got 81.3% and is the best Smartphone OS in the world today.

In 2014, Arshad et. al. [8], planned a light weight taint analysis tool for android application named AT2. This tool achieved static analysis on android applications (APKs) using reverse engineering techniques and taint-aware slicing. To examine the structure of an application, it utilized program slicing technique for data flow analysis. It executed the program slicing on full class name and procedures name of an android application. The information leakages were noticed using taint analysis technique on sliced programs. At the end, it offered a user friendly detailed report of study done on android applications (APKs); which assisted to increase the security of android applications.

In 2013, Ahmed et. al. [9], contrasted two most popular mobile operating system android and iOS in terms of safety. They compared security features like Encryption, Data Storage Format, Application Sandboxing, Memory Randomization, and Built-in Antivirus in both Mobile OS. From contrast, they decided that iOS is more safe than android OS. They also designated some security points to save the user- sensitive data safe on the respective Smartphones.

In 2013, Sharma et. al. [10], debated about the various mobile technologies like 1G, 2G and 3G along with the various mobile phones based on different OS available in the market.
They chiefly compared Symbian OS, BlackBerry OS, Android OS, iOS and Windows Phone according to Vendor, Programming Language and Application Store. They also distinguished iPhone from blackberry and Symbian. From the variance, they found that iPhone has more attributes and involve less code to write its application. Because of this, iPhone causes fewer bugs. At the end, they decided that android and apple are growing at a fast speed in the market.

In 2013, Johnson et. al. [11] offered a framework for enlightening the software security, functionality and accessibility dangers for handheld devices. This framework implemented all the probable execution paths without any form of user input; as well as libraries by means of static as well as dynamic code analysis. The output of static code analysis was utilized as an input for the execution of dynamic code analysis. A large number of android applications are tested to show its functionality and feasibility. This approach can be utilized for other purposes like program confirmation, mnemonic execution, coactive debugger and deep exploration of an android application.

In 2012, Nosrati et. al. [12], presented a brief outline of mobile computing including various mobile devices and operating systems. The devices like tablet, smartphone, personal digital assistant, ultra-mobile PC, and wearable computers are presented. They also conversed about BlackBerry, iOS, Android, and Bada, Symbian, Windows, Palm OS. At the end, some common drawbacks of mobile computing devices are exposed.

In 2011, Becher et. al. [13], discussed about security of mobile devices. They distinguished security of handheld devices from computer system. They also categorized attacks for smartphones in four groups hardware-related, device independence, software-related, and user-centric. They concluded that the smartphones are increasing swiftly as compared to regular computer in terms of processing power, display size, and versatility of operating systems. As an upshot, mobile security becomes a fascinating field.

In 2011, Jaeyeol et. al. [14], discussed that Smartphone using application like Android, BlackBerry, Linux and iPhone that satisfy the user requirements has become a requirement. They over-reviewed the associated work about media player for audio-video files, Handler, SD card for storage and activity life cycle of android application. From review, they projected the class diagram for English tutoring application, handler function and Text-to-Speech. At the conclusion, they proposed optimization function to develop English tutoring android application for user to learn English without difficulty in a expectation that it will aid developers to write English applications.

This work is licensed under a Creative Commons Attribution 4.0 International License.
In 2010, Wu et al. [15], discovered that android platform can be stretched as an educational tool. They defined sheep framework for game development by extending android platform centred on previous students’ projects. From the conversation, they discovered that they can apply or increase a tool to grasp software architecture course using double simulation method that is to permit the second stimulus that rival the first stimulus.

In 2009, Lin et al. [16], examined the smartphone OSs market under a uniform ecosystem framework. They first compared “food webs” of major companies like Nokia, Apple, RIM and Microsoft. From the evaluation, they found that companies use smartphone OS just as a business unit and utilize it as a chance for new business. For competition among diverse OS device maker and application developer are two key factors and authenticate them with network effect theory.

The mobile operating system utilized for various handheld devices like smartphones, tablets, PDAs, or other mobile devices. In latest past, the research activities are focused in areas like contrast of various mobile operating systems, security of personal data, reverse engineering of mobile based application. The analysis shows that android and iPhone are most common operating system among all other smartphone OS. Most of the security techniques do not tolerant to malevolent activities in smartphones.

4. COMPARISON OF DIFFERENT SMARTPHONES

Mobile Devices i.e. handheld devices have become a crucial part for communication purpose in human being’s life. Because of change in technology and time, use of mobile devices moved towards to Smartphones. In existing work, the authors basically make contrast between smartphone based operating system like android, iPhone, blackberry and Symbian. Moreover, we also have analysed about other latest operating system like window phone, webOS, Ubuntu and firefox. We have shown the comparison in table 1. This graphical presentation will help to easily differentiate among different operating systems. Some characteristics of different smartphones OS have been evaluated. The contrast result helps to recognize various results by comparing different smartphone based operating system that is shown in Table 1.
Tabel 1: Comparison of different Smartphones operating System [1, 6, 8, 11, 13]

<table>
<thead>
<tr>
<th>OS Parameter</th>
<th>Android</th>
<th>IOS</th>
<th>Symbian</th>
<th>Blackberry</th>
<th>Windows Phone</th>
<th>WebOS</th>
<th>Ubuntu</th>
<th>Firefox</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Family</td>
<td>Linux</td>
<td>Darwin</td>
<td>RTOS</td>
<td>QNX Window CE-7</td>
<td>Window NT-8</td>
<td>Linux</td>
<td>Linux</td>
<td>Linux</td>
</tr>
<tr>
<td>Vendor</td>
<td>Open Handset Alliance, Google</td>
<td>Apple, Inc</td>
<td>Accenture on behalf of Nokia (historically Symbian Ltd. and Symbian Foundation)</td>
<td>Blackberry Ltd.</td>
<td>Microsoft</td>
<td>Open WebOS community contributors LG Electronic, previously HP(HeWlett-Packard) &amp; Palm</td>
<td>Canonical Ltd. Ubuntu community</td>
<td>Mozilla Foundation</td>
</tr>
<tr>
<td>SDK Platform</td>
<td>Linux, Mac OS X and Windows</td>
<td>Mac OSX using iOS SDK</td>
<td>Windows XP Professional SP2; Vista &amp; 7 for some SDRs</td>
<td>Linux, Windows, Mac OS X</td>
<td>Windows</td>
<td>OS X, Ubuntu, Windows</td>
<td>Ubuntu Desktop using Ubuntu SDK</td>
<td>All where Firefox is available</td>
</tr>
<tr>
<td>CPU Architecture</td>
<td>ARM, x86, MIPS</td>
<td>ARM, ARM 64</td>
<td>ARM, x86</td>
<td>ARM</td>
<td>ARM</td>
<td>ARM and x86</td>
<td>ARM, x86</td>
<td></td>
</tr>
<tr>
<td>Source Model</td>
<td>Open source and in most devices with proprietary components</td>
<td>Closed source</td>
<td>Closed source, previously open source</td>
<td>Closed Source</td>
<td>Closed Source</td>
<td>Open Source</td>
<td>Open Source</td>
<td>Open source</td>
</tr>
<tr>
<td>License</td>
<td>Free and open-source, but usually bundled with proprietary apps and drivers</td>
<td>Proprietary EULA except for open source components</td>
<td>Proprietary, previously licensed under EPL</td>
<td>Proprietary</td>
<td>Apache License</td>
<td>Free and open-source, mainly theGPL</td>
<td>Free and open-source, mainly theMPL, Apache</td>
<td></td>
</tr>
<tr>
<td>Latest Release (2014)</td>
<td>5.1 &quot;Lollipop&quot; / March 10, 2015; iPhone 6 Plus/ September 18, 2014;</td>
<td>Nokia Belle Feature Pack 2 / October 2, 2013; BlackBerry 9790/9900/ November 2013; Windows Phone 8.1 Update / December 5, 2014;</td>
<td>2.2.4 (Pre 3) (phone) / January 12, 2012; 14.10 Utopic Unicorn / October 2014</td>
<td>1.4.0/ August 8, 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This work is licensed under a [Creative Commons Attribution 4.0 International License](http://creativecommons.org/licenses/by/4.0/).
5. CONCLUSIONS AND FUTURE SCOPE

Smartphones like personal computer offers numerous functions like use of application, usability, web browsing, running GPS, expendable memory; multitasking, multiprocessing, playing games, social networking etc. In this paper, we have offered a detailed review and comparative study of various Smartphones operating systems. We have made contrast between android, iOS, Symbian, Blackberry, Windows Phone, WebOS, Ubuntu and Firefox.

For comparison, various factors of existing work like OS family, IDE, GUI, SDK platform, CPU Architecture, etc. and some new factors like Market Size, Market share, Debugger availability, Cross platform deployment, Reverse Engineering tool, future Scope etc. have been taken into account. Because these factors offer new research inclinations of smartphone based operating systems.

From comparative analysis and market share analysis during fourth quarter of 2014, we have discovered that android and Windows Phones are superior to others OS. Android gets 80.7% and is the finest Smartphone OS in the world today. We can also utilize it as an Educational tool. Due to android as an open source operating system, the user can effortlessly install third party applications from markets and even from unreliable sources. Due to this, it has some restrictions which lead to malware attacks like virus, worms, spyware, adware and Trojan horse. So, we propose detection of malware before installation of an application as well as comparison of android, iOS, Symbian, Blackberry, Windows Phone, WebOS, Ubuntu and Firefox Smartphones OS in terms of security.

ACKNOWLEDGMENTS

Our thanks to each and every person who contributes in any ways to complete this research work helps to recognize various results by comparing different smartphone based operating system that is shown in Table 1.

REFERENCES


[10]. Ahmad, M. S., Musa, N. E., Nadarajah, R., Hassan, R., & Othman, N. E. (2013, July). Comparison between android and iOS Operating System in terms of security. In Information Technology in Asia (CITA), 2013 8th International Conference on (pp. 1-4). IEEE.


