A Study on Smartphone based Operating System

Kiran Bala  
M.tech Student,  
CSE department,  
Chandigarh University,  
Gharuan, Mohali, India

Sumit Sharma  
Assistant Professor,  
CSE department,  
Chandigarh University,  
Gharuan, Mohali, India

Gurpreet Kaur  
Assistant Professor,  
CSE department,  
Chandigarh University,  
Gharuan, Mohali, India

ABSTRACT
At present there are many mobile phones operating systems available in the market but mobile phones with android OS have now become domestic product which was once extravagant product. The reason towards this change is attributed to its varied functionality, ease of use and utility. There are number of tasks performed on it like making call, sending or receiving SMS, music, billing, online shopping, online booking, playing games, web browsing, using different apps like whatsapp, facebook or Applock etc. Hence a large amount of user sensitive data is stored within the devices [1]. Increased usage of smartphone has led towards higher concerns about security of user-private data. Due to android as an open source mobile platform, user can easily install third party applications from markets and even from unreliable sources [2]. Thus, Android devices are a soft target for privacy intrusion. Whenever the user wants to install any application, firstly it’s the description and the application screenshots which provides an insight into its utility. The user reviews the description as well as a list of permission requests before its installation. As the types and rate of malicious attacks increases, the difficulty of examining in advance whether an app is malicious or not through its descriptions has increased manifolds. In this paper we have reviewed and examined android software stack and compared smartphone based operating system like android, iOS, blackberry, Symbian, windows phone, webOS, Ubuntu and firefox.

General Terms  
Android, Operating System and Security

Keywords  
Android software architecture; android; iOS; Symbian; blackberry; windows phone; webOS; Ubuntu; Firefox; Android Security.

1. INTRODUCTION
Smartphones are now participating nearly in each and every sphere of life like business, education, workplace and healthcare. The Worldwide Mobile Communications Device Open Operating System Sales (WMCDOS) provides total market of 104,898 to End Users by OS [3]. There are over 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 developed it for handset manufacturers like T-Mobile, Sprint Nextel, Google, Intel, Samsung, etc. [1]. It offers to consumers a richer, less expensive, better mobile experience and various features like 3D, SQLite, Connectivity, WebKit, Dalvik and FreeType etc. Since android provides open source operating system; users and developers can get source code but only under the rules and conditions [1].

Whenever the user wants to install any application, firstly its description as well as a list of permission requests is provided with an opportunity for review before its installation or cancel the installation if he or she finds that the permissions are too many or objectionable. The android operating system has its own well established android permission model, but intruders can supplements them by allowing the components to be changed within and across the applications through Intent communication mechanism due to which it has susceptibility for attacks by malwares [5].

Android open source platform requires strong and complex security architecture to ensure security of user private data, personal information, application and network, but it has few constraints for developers which raises the security risk for the end users [2].

This paper is to compare the latest smartphone operating system like android, iOS, blackberry, Symbian, windows phone, webOS, Ubuntu and firefox. The comparison between different smartphone operating system is done using different parameters like OS family, Environment and market share. After summing up findings through the comparison, the conclusion discuss which operating systems are in competition and draw some conclusions 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 form of different layers of stacked as software that comprises 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 tightly integrated and provides 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 consists of different layers that provide 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  
Applications using standard Java programming are all other operating systems. Custom alerts in the status bar described the Android architecture, user and contact management, debugging and development, security, isolation, memory compilation, improved garbage collection, improved virtual machine separately.

Android applications are at the topmost layer of the architecture, which leads to malware attacks environment within which they are constructed from reusable, higher-order components. It provides many packages of higher-level services to application that collectively form the environment within which they are constructed from reusable, interchangeable and replaceable components. It provides the functions of phone like location management, data sharing, resource management etc.

The packages present are as given below:

2.4.1 Activity manager
It controls and manages the activity lifecycle of applications.

2.4.2 Resource manager
It manages and provides access to non-code embedded resources such as graphics, strings, color settings and user interface layouts.

2.4.3 Notification manager
It allows all applications to show custom alerts in status bar and notifications to the user.

2.4.4 Location manager
When user enters or leaves 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 layer of the Android software stack. These comprise both the native applications and the third party applications. The native applications provide the basic Android implementation such as SMS client app, Dialer, Web browser and Contact manager. The third party applications are further installed by the developers, programmers while debugging/testing and user after purchasing the device.

3. RELATED WORK
As android usage are increasing day by day, so android have emerged as an outstanding area of research in recent past. Research activities are concentrated in areas such as reverse engineering, clustering, machine learning, operating system and security and they have received a lot of attention. Since the proposed work is focused on operating system and security, this survey 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 key features. They also compared Android with different OS like iOS (Apple), Symbian (Nokia) & Blackberry OS (RIM). From their survey, they concluded that android is better than all other operating systems. However due to open source OS and unique features, android has some limitations which leads to malware attacks like virus, worms, spyware, adware and Trojan horse.
In 2014, Okediran et. al. [6], presented a review and comparative analysis of different technological platforms. They mainly reviewed six Smartphone based OSs like Android-Google, iOS-Apple, Windows Phone-Microsoft, Blackberry OS, webOS and Symbian OS-Nokia. They found that Android can run on all mobile devices becomes the most popular operating system all over the world in the world ever.

In 2014, Dabhi et. al. [7], presented a detail review on latest and upcoming operating systems like IOS 7(Apple), Android 4.4 KitKat (Google) and windows 9 (Microsoft). They compared updated features, facilities, performance and verdict about these operating systems. From market share analysis during December 2013, They found that Android got 81.3% and is the best Smartphone OS in the world today.

In 2014, Arshad et. al. [8], proposed a lightweight taint analysis tool for Android application named AT2. This tool performed static analysis on Android applications (APKs) using reverse engineering techniques and taint-aware slicing. To analyze the structure of an application, it used program slicing technique for data flow analysis. It performed the program slicing on full class name and methods name of an Android application. The information leaked were detected using taint analysis technique on sliced programs. At the end, it presented a user friendly detailed report of analysis performed on Android applications (APKs); which helped to enhance the security of Android applications.

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

In 2013, Sharma et. al. [10], discussed about the various mobile technologies like 1G, 2G and 3G along with the different mobile phones based on different OS available in the market. They mainly compared Symbian OS, BlackBerry OS, Android OS, iOS and Windows Phone according to Vendor, Programming Language and Application Store. They also differentiated iPhone from blackberry and Symbian. From the difference, they found that iPhone has more features and requires less time to write its application. Due to this, iPhone causes fewer bugs. At the end, they concluded that Android and apple are growing at a fast pace in the market.

In 2013, Johnson et. al. [11] presented a framework for revealing the software security, functionality and accessibility risks for handheld devices. This framework executed all the possible execution paths without any kind of user input; as well as libraries using static as well as dynamic code analysis. The output of static code analysis was used as an input for the execution of dynamic code analysis. A large number of Android applications are tested to display its functionality and feasibility. This approach can be used for other purposes like program confirmation, memory execution, coactive debugger and deep exploration of an Android application.

In 2012, Nosrati et. al. [12], presented a brief introduction 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 introduced. They also discussed about BlackBerry, iOS, Android, and Bada, Symbian, Windows, Palm OS. At the end, some general limitations of mobile computing devices are subjects.

In 2011, Becher et. al. [13], discussed about security of mobile devices. They differentiated security of handheld devices from computer system. They also classified attacks for smartphones in four categories hardware-related, device independence, software-related, and user-centric. They summarized that the smartphones are growing rapidly as compare to ordinary computer in terms of processing power, display size, and versatility of operating systems. As a result, mobile security becomes an interesting area.

In 2011, Jaeyeol et. al. [14], discussed that Smartphone using application like Android, Blackberry, Linux and iPhone that fulfill the user requirements has become a prerequisite. They over-reviewed the related work about media player for audio-video files, Handler, SD card for storage and activity life cycle of android application. From survey, they proposed the class diagram for English tutoring application, handler function and Text-to-Speech. At the end, they proposed optimization function to develop English tutoring android application for user to learn English easily in a hope that it will help developers to write English applications.

In 2010, Wu et. al. [15], found that android platform can be extended as an educational tool. They described sheep framework for game development by extending android platform based on previous students’ projects. From the discussion, they found that they can apply or expand a tool to grasp software architecture course using double simulation method that is to enable the second stimulus that rival the first stimulus.

In 2009, Lin et. al. [16], analyzed 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 comparison, they found that companies use smartphone OS just as a business unit and use it as an opportunity for new business. For competition among different OS device maker and application developer are two key factors and validate them with network effect theory.

CONCLUSION

The mobile operating system used for various handheld devices like smartphones, tablets, PDAs, or other mobile devices. In recent past, the research activities are concentrated in areas like comparison of various mobile operating systems, security of personal data, reverse engineering of mobile-based application. The analysis show that android and iPhone are most popular operating system among all other smartphone OS. Most of the security techniques do not tolerant to malicious activities in smartphones.

4. COMPARISON OF DIFFERENT SMARTPHONES

Mobile devices i.e. handheld devices have become an important part for communication purpose in human being’s life. Due to change in technology and time, use of mobile devices shifted towards to Smartphones. In existing work, the authors basically make comparison between smartphone based operating system like android, iPhone, blackberry and Symbian. In addition to it, we also have discussed about other recent operating system like window phone, webOS, Ubuntu and firefox. We have presented 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 comparison result helps to identify different results by comparing different smartphone based operating system that is shown in Table 1.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>OS Family</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</td>
<td>Linux</td>
<td>Darwin</td>
<td>RTOS</td>
<td>QNX</td>
<td>Window CE-7</td>
<td>Linux</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 Electronics, previously HP (Hewlett-Packard) &amp;Palm</td>
<td>Canonical Ltd. Ubuntu community</td>
<td>Mozilla Foundation</td>
<td></td>
</tr>
<tr>
<td>SDK Platform</td>
<td>Linux, Mac OS X and Windows, using iOS SDK</td>
<td>Windows XP Professional SP2; Vista &amp; 7 for some SDKs</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>
<td></td>
<td></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>
<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>Open Source</td>
<td>Open Source</td>
<td>Open source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>License</td>
<td>Free and open-source, but usually bundled with proprietary apps and drivers</td>
<td>Proprietary EUL, 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>
<td></td>
</tr>
</tbody>
</table>

TABLE 1. Comparison of different smartphone operating system[1, 6, 8, 11, 13]
<table>
<thead>
<tr>
<th>OS</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>Package Manager</td>
<td>Google Play, APK</td>
<td>iTunes</td>
<td>Nokia Store</td>
<td>BlackBerry Link</td>
<td>Zune Software (not since Windows 8)</td>
<td>OTA deployment, webOS through App store, Web URL, Precentral, .apk</td>
<td>Ubuntu Touch through App store, Web URL</td>
<td>Firefox OS Packaged Apps</td>
</tr>
<tr>
<td>Runs On</td>
<td>Smartphones, tablet, computers, TVs, cars and wearable devices</td>
<td>iPhone, iPad, iPod Touch</td>
<td>Smartphones</td>
<td>Smartphones</td>
<td>personal computers, smartphones, server computers and embedded devices</td>
<td>TVs and Smart watches</td>
<td>Personal computers, Servers, smartphones, tablet computers (UbuntuTouch), smartTVs (Ubuntu TV)</td>
<td>Smartphones, Tablet and computers</td>
</tr>
<tr>
<td>Market Share</td>
<td>48.8%</td>
<td>17.2%</td>
<td>0.1%</td>
<td>11.1%</td>
<td>19.5%</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Market Size</td>
<td>Very High</td>
<td>High</td>
<td>Very low</td>
<td>Low</td>
<td>Medium</td>
<td>Very low</td>
<td>Very low</td>
<td>Very low</td>
</tr>
<tr>
<td>Non-English Language Support</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Debugger</td>
<td>Debugger available</td>
<td>Debugger available</td>
<td>Debugger available</td>
<td>Debugger available</td>
<td>Debugger available</td>
<td>Debugger available</td>
<td>Debugger available</td>
<td>Debugger available</td>
</tr>
<tr>
<td>Cross-Platform Deployment</td>
<td>Android only</td>
<td>iPhone, iPad, iPod Touch</td>
<td>Compile per target</td>
<td>BlackBerry only</td>
<td>Windows Mobile, Windows FU, Windows CE</td>
<td>webOS, Palm only</td>
<td>HTML5 app to be av*ailable web browser.</td>
<td>Web browser on other platform</td>
</tr>
<tr>
<td>GUI</td>
<td>Android</td>
<td>Cocoa Touch</td>
<td>Avkon</td>
<td>Cascades</td>
<td>Visual Studio</td>
<td>Graphical (Luna)</td>
<td>Ubuntu SDK</td>
<td>Firefox browser, Firebug</td>
</tr>
<tr>
<td>Tool for Reverse Engineering of App</td>
<td>Apk tool, Dex2jar, JD-Compiler, XDA Auto tool</td>
<td>iREF Toolkit, Windows Explorer, oTool, iExplorer, Class-dump-z</td>
<td>Carbidge.c++, JDA Pro, APP Trk, SISWare, ARM assembler</td>
<td>JD-GUIL, Ntoppad, VSMTool, COD extractor</td>
<td>Decompressor, Visual Studio / Notepad, .Net Decompiler</td>
<td>Binwalk</td>
<td>Bokken</td>
<td>gdb-debbuger, b2g-ps</td>
</tr>
<tr>
<td>Future Prospect</td>
<td>Very High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Note:**
- "Very High" Market Share
- "Very High" Market Size
- "High" Application Store
- "High" Document At
- "Medium" Future Prospect
- "High" Tool for Reverse Engineering of App
5. CONCLUSIONS AND FUTURE SCOPE
Smartphones like personal computer provides various functionalities like use of application, usability, web browsing, running GPS, expendable memory; multitasking, multiprocessing, playing games, social networking etc. In this paper, we have presented a detail review and comparative analysis of different Smartphones operating systems. We have made comparison between android, iOS, Symbian, Blackberry, Windows Phone, WebOS, Ubuntu and Firefox.

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

From comparative analysis and market share analysis during fourth quarter of 2014, we have found that android and Windows Phones are superior to others OS. Android gets 80.7% and is the best Smartphone OS in the world today. We can also use it as an Educational tool. Due to android as an open source operating system, the user can easily install third party applications from markets and even from unreliable sources. Due to this, it has some limitations 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.

6. ACKNOWLEDGMENTS
Our thanks to each and every person who contributes in any ways to complete this research work.

7. REFERENCES