

The Most Secure Smartphone Operating System: A Survey

Sundus Ayyaz, Saad Rehman

Abstract—In the recent years, a fundamental revolution in the Mobile Phone technology from just being able to provide voice and short message services to becoming the most essential part of our lives by connecting to network and various app stores for downloading software apps of almost every activity related to our life from finding location to banking from getting news updates to downloading HD videos and so on. This progress in Smart Phone industry has modernized and transformed our way of living into a trouble-free world. The smart phone has become our personal computers with the addition of significant features such as multi core processors, multi-tasking, large storage space, bluetooth, WiFi, including large screen and cameras. With this evolution, the rise in the security threats have also been amplified. In Literature, different threats related to smart phones have been highlighted and various precautions and solutions have been proposed to keep the smart phone safe which carries all the private data of a user. In this paper, a survey has been carried out to find out the most secure and the most unsecure smart phone operating system among the most popular smart phones in use today.

Keywords—Smart phone, operating system, security threats, Android, iOS, Balckberry, Windows.

I. INTRODUCTION

THE growth in the Smartphone industry took its pace in 2010 and is still growing at amazingly faster rate that the present high tech phones will be considered obsolete in near future. The Smartphone operating system is responsible for running various services on the phone such as making call, sending messages, internet browsing, app downloading and so on [1], [2]. The Smartphone Operating System not only supports various features of a complete computer system such as high speed central processing units (CPU) and graphics processing unit (GPU), large storage space, multitasking, high-resolution screens and cameras, multipurpose communication hardware but also combine other features including a touch screen, cellular, Bluetooth, Wi-Fi, global positioning system (GPS) mobile navigation, video camera, voice recorder, music player, near field communication and infrared blaster [6]. For supporting such distinct features, the Smartphone OS possess very complex architecture.

Modern Smart phones are designed in such a way that they can support any software (mobile app) written by external application developers. This feature allows the users to add new apps and services to their mobile by simply downloading them from software developers' application stores e.g. Apple's 'App Store', Google's 'Android Market', Blackberry's 'App

World', Windows Mobile's 'Windows Market place' and so on. This feature of smart phone devices provides one of the utmost advantage for users by allowing them to connect to various applications and services [6].

Smart phones show the competence to maintain the features of a traditional mobile phone system as well as the computer system by running different application programs (mobile apps). Mobile apps being distributed from the mobile app store such as Google Play and Apple Store drives the smart phones by providing a mobile app ecosystem. There is almost every mobile app available focusing different aspects of a user's life. Due to the emergence of app store ecosystem, the dependency of a mobile user for services such as messaging and data services on Mobile Network Operator(MNO) has been disrupted as most of the important services are now easily provided by the mobile app stores such as the mobile app called 'Whatsapp' which provides the text services has replaced the SMS text by providing a direct route to market without any intervention of MNO [1]. For using these value added services without the intrusion of MNO, smart phone users are exposed to various security risks. By considering the four most popular smart phone operating systems; Android, iOS, Blackberry OS and Windows phone, this paper shows a survey of four most practical smart phone OS at the present time to evaluate the most secure operating system between all by analyzing different factors in their OS which makes them vulnerable to security hazards.

II. SMARTPHONE OPERATING SYSTEMS

Mobile apps also called the application programs needs a software platform on which they can run. Such platform is called Mobile Operating System (Mobile OS). In the past decade, the OS have gone through 3 phase evolution from PC-based OS to an embedded OS and the present smart phone oriented OS [6]. The four most important smart phone operating systems are Android, iOS (iphone/ipod/ipad), Blackberry and Windows Phone. In 2011, the Symbian smart phones were considered most popular as they were being sold worldwide than any other phone but today the Nokia has replaced its Symbian OS with Wondows Phone [7]. The table demonstrated in Fig. 1 shows the 4th Quarter smart phone shipments of three years from 2012-2014. We can observe that the most shipments are made for Android phones around 77% in 2014 then comes the iOS with 20% while windows phone carry 3% of total shipment and the blackberry with less than 1 percent.

Sundus Ayyaz is with the National University of Sciences and Technology, Pakistan (e-mail: sundus.ayyaz@ceme.nust.edu.pk).

**GLOBAL 4TH QUARTER SMARTPHONE SHIPMENTS
 (From IDC - percentages Rounded)**

| Platform | 4Q12 | 4Q13 | 4Q14 |
|---------------|------|------|------|
| Android | 70% | 78% | 77% |
| iPhone (iOS) | 21% | 18% | 20% |
| BlackBerry | 3% | <1% | <1% |
| Windows Phone | 3% | 3% | 3% |
| Other | 3% | 1% | <1% |

Fig. 1 4th Quarter smart phone shipments of three years from 2012-2014

Following is the brief introduction of the popular smart phone operating systems;

A. Android OS

Android is a Linux based operating system developed by Google in combination with the open hand alliance [8]. In 2008, the first Android smart phone was launched and it became the major competitor of iPhone due to its support from smart phone manufacturers as well as multiple carriers. One of the most popular feature of Android phones is its large screen e.g. phablet. In 2011, Android outperformed every other smart phone in market. While in 2013, Google play store published more than 1 million Android apps which are collectively being downloaded 50 billion times. Correspondingly, according to a survey conducted in 2013, among the mobile developers 71% of them are Android developers [6]. There are four layers in Android platform, the Linux Kernel, which is responsible for security, process and memory management. The Android runtime, C/C++ Android Libraries and Application Framework.

B. iOS

iPhone Operating System is a Unix based OS. It was first launched in 2007 by the Apple Inc to support Apple devices such as iPhone, Ipad, Ipod touch and Apple TV. Unlike Android, iOS does not support installation on non-Apple hardware. In 2012, Apple store contained more than 700,000 iOS applications and the download of over 30 billion apps are recorded. There are four abstraction layers in iOS, the core OS layer, the core services layer, the media layer and the cocoa touch layer [6], [8].

C. Blackberry OS

Blackberry OS is designed and developed by Research in Motion (RIM). First Blackberry smart phone was launched in 1999 but the advanced blackberry devices were introduced in 2011. The blackberry devices include personal digital assistants, portable media players, internet browsers, gaming devices, cameras etc. [8]. One of the major strengths of Blackberry OS is their ability to handle corporate emails while maintaining a high level security through on device message encryption. BlackBerry OS supports two protocols, the Java

Mobile Information Device Profile (MIDP) and the Wireless Application Profile (WAP) which synchronize through BlackBerry Enterprise Server (BES). The BES is responsible for providing different features, one of them is the security for mobile devices [6], [8]. According to one survey conducted in 2011, around 3% of blackberry devices were sold worldwide making RIM the sixth most popular device manufacturer. The blackberry internet service is available in 91 countries around the world and according to a study, in October 2011, there were seventy million subscribers to blackberry worldwide.

D. Windows OS

An Operating System developed by Windows for embedded systems. It is also abbreviated as WinCE [8]. It was released in 2010 with the name Windows Phone 7. Different hardware manufacturers such as Samsung, LG, Nokia and HTC are developing Windows Phone devices. In 2011, Windows Phone 7 obtained a major upgrade known as 7.5 Mango by adding features to the original design and it is declared as the main OS for all Nokia smart phones in future. Windows 8 was released in 2012 known as second generation [6]. The recent version of Windows Embedded Compact supports Intel x86 and compatibles, MIPS, and ARM processors [8].

E. Smartphone Operating Systems and the Market Share

According to 2015 market share as illustrated in Fig. 2, the most popular OS among the major OS is Android which holds 44% of the total share in smart phone industry, next popular is Windows with 20% share and then comes the iOS and blackberry with 17% and 13% correspondingly.

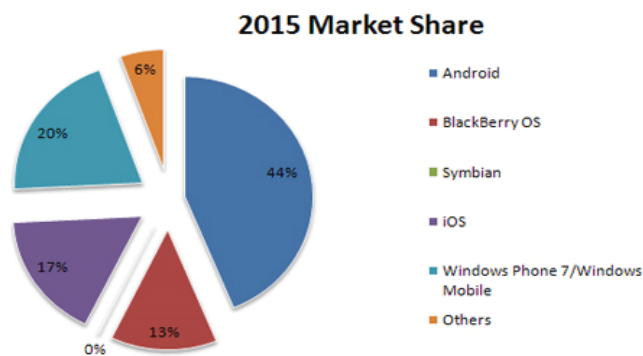


Fig. 2 Smart Phone Market Share 2015

F. Smartphone Security Threats

In the last few years, the security threats have been grown so much that the top most stories regarding smart phones are concerned with their security violation, mobile malware and the hacking of cloud services in different ways. As the cloud services such as iCloud, Google Drive and Dropbox are being closely incorporated in our smart phones, we started to pour more and more digital data into our phones which eventually occupy most of our phone's memory. As many of us are not aware of the potential security threats associated with our phones, we have used our phones to store our personal and sensitive information such as emails, personal messages, bank account details, passwords and pictures in addition to the

location and contact details [4]. These are all transparent in our phones that we cannot even afford it to get stolen or being effected by harmful viruses such as malware and Trojan horses which can hack the data causing financial fraud and personal information loss [2]. Every smart phone platform is exposed to threat, no matter what OS a person is using. Some OS are safer as compared to others but none are protected [3]. Every mobile user wants their information to remain secure and not misused as they place their trust on various app stores for downloading different apps on their phones as well as on the hardware manufacturers and mobile networks [4], [5].

The most common security threats and vulnerabilities of smart phones are, Phone stolen or lost causing loss of private data and identity, Financial Fraud, Privacy Loss due to spyware or malware, Banking Fraud [2]. Almost every smart phone has its own risks when it comes to hackers or malware [5].

G. Most Secure Smart Phone OS- A Comparison

A Survey have been carried out in this paper to find the safest of the four most popular OS in use today (Android, iOS, Blackberry and Windows Phone).

According to [3], one of the main reasons for Smartphone security issues is the unawareness among mobile users. Consumers should be educated enough to understand the risk of their phone to be stolen or lost when they have stored sensitive data such as bank details and passwords on their phones. In recent years, a multi-billion-pound cybercrime industry organized by some crime groups have developed Malware, which steal the data on phone silently. According to [3], Android is considered as the most unsecure OS, therefore, an AndroidBouncer feature is added in android based phones which is used to check the malicious apps. The users of smart phones are also recommended to read and accept the

download privileges undoubtedly before downloading an app especially when updating it that the manufacturer haven't added any feature they shouldn't have. In 2014 an analysis conducted by Kaspersky Labs [4], showed that adware is considered the most widespread mobile malware devastating around 26.7% of mobile devices. Trojan SMS is another one. These viruses continue to harm our personal and financial information in different ways. In the next version of Android ("Lollipop"), Google has included important security features by default such as improved lock screen, encryption and Device Manager features to track the stolen device. By taking few sensible precautions, a user can avoid security threats to some extent such as avoid downloading of untrusted apps, keeping a strong password to lock the phone and avoid keeping sensitive information such as bank details in phone. Modern device manufacturers are adding biometric sensors such as fingerprint scanners for increasing the smart phone security. A survey conducted by Security Firm Checkpoint [9] by interviewing 768 IT Professionals from USA, UK, Canada, Germany and Japan demonstrated that Apple's iOS is the most secure OS to be used in corporate environments while Google's Android is considered the less secure among all OS. A security enhanced version of Android is also being released to solve different security issues. According to a report from 2014 [10], 97% of Mobile Malware is on Android. Android being the most popular and holding a great place in Global Smart Phone Market, it has more security threats than any other platform. One way to stay safe on Android is to only download apps from Google Play Store as the most of Mobile Malware enters from unregulated third party app store.

Table I shows the study of different articles and papers to discover the most secure Smart Phone OS.

TABLE I
 SECURITY COMPARISON OF DIFFERENT SMART PHONE OS FROM LITERATURE

| Articles: | Smart Phone Operating Systems | | | | Result |
|-----------|---|--|---|---|---|
| | Android | iOS | Blackberry | Windows | Safest to Exploited |
| [3] | Less mature, doesn't control the eco-system properly, Open-source, downloading app from external source, different devices use them | Strong control on eco-system, Tight control on hardware, software and applications. | RIM being an Enterprise vendor. Most mature, Stable and Enterprise Friendly. | Supports Security features such as sandboxing, buffer overflow prevention and not having a file system. | 1) Blackberry 2) iOS 3) Windows 4) Android |
| [4] | Encryption is off by default, high market share then iOS, built in virus protection in most devices. | Encryption by default in iOS 8. | | | 1) iOS 2) Android |
| [5] | Easier Target for hackers due to PC OS structure Google Play is built on open model | Secure Sandbox configuration | Encryption software is employed to protect data. | | 1) Blackberry 2) iOS 3) Android |
| [9] | Only 21% of Android devices holds connections in corporate setting, less secure among all platforms | Most common OS to be connected in corporate environments e.g. 30% iOS devices are connected. | 29% of Blackberry devices are connected in business environments. | 18% of total connected devices have Windows OS. | 1) iOS 2) Blackberry 3) Windows 4) Android |

A few of the latest articles related to smart phone OS and devices have been studied and analyzed in different ways to

find out the most secure smart phone platforms in use today. According to Table I, it is analyzed that Android is the most

unsecure OS with being the most popular among users while Blackberry and iOS are considered the Secure ones with the reasons given consequently for the use in Corporate Business environments while iOS holds the position of being the most secure OS among all others in use today.

III. CONCLUSION

The emergence of various competing Smart Phones platforms have enforced the device manufacturers to provide the value added services and struggle for the most popular as well as the most secure Smart Phone Operating System (OS) provider in the Market. With respect to the Smart Phone OS, Google's Android has been considered the most popular among users worldwide as it can run on all mobile devices such as Samsung and Huawei Sets but it has also been declared as most unsecure. While Blackberry and iOS are analyzed to be having most secure OS to be connected and used in business environments. A survey has been conducted in this paper following different reasons and conditions of each Mobile OS, the four most popular Smart Phone devices in use today are rated from safest to exploited as depicted in Table I.

REFERENCES

- [1] Tamura (2013), "Device Connectivity Technologies using Short Distance Wireless Communications."
- [2] Goode Intelligence (2015), "Study into the Implications of Smart Phone Operating System Security."
- [3] David Gilbert (2012) " How Secure is your Smart Phone? Android, iOS, Blackberry and Windows Phone under attack."
- [4] Roland Banks (2014), "Smart Phone Security-- What's the Risk?"
- [5] Robert Leedham (2013), "Smart Phone Security-- How to Protect your Mobile?"
- [6] Okediren O. (2014), "Mobile Operating Systems and Application Development Platforms: A Survey" published in Journal of Advancement in Engineering and Technology.
- [7] Smart Phone Operating Systems <http://www.pcmag.com/encyclopedia/term/63006/smartphone-operating-system>
- [8] Masoud Nosrati, Ronak Karimi, Hojat Allah Hasanvand (2012), "Mobile Computing: Principles, Devices and Operating Systems" published in WAP Journal.
- [9] M Usman Butt (2012), "Corporations prefer iOS over Blackberry and Android for Security Purposes."
- [10] Gordon Kelly (2014), "Report: 97% of Mobile Malware is on Android."