# Smartphone and Security Challenges

**Ahmad Vakil**
Department of Computer Information Systems/Decision Sciences
St. John's University
Queens, NY 11439, USA.

**Manuel Russon**
Department of Computer Information Systems/Decision Sciences
St. John's University
Queens, NY 11439, USA.

## Abstract

*With the increase in popularity of smartphones around the world during the last 10 years, users of these devices face a tremendous challenge in order to access, store and spread information safely. New smartphones have become more and more powerful and, as a result, users of such devices utilize them to process more sensitive personal, financial, and even corporate information. The huge amount of information and the quality of such information processed by these devices, presents us with an extremely challenging security task. Indeed, smartphone security threats are making headlines every day. In this study, we first examine major trends in mobile computing. Then we examine major vulnerabilities of these devices. Indeed, it can be said that no Smartphone operating system is totally safe. Finally, we propose several methods to reduce the security vulnerabilities of these devices.*

**Keywords:** Operating System, Android, iOS, Security Vulnerability.

## *1. Introduction*

While the smartphone has been around since 1990's, the introduction of iPhone in 2007 created a massive demand at the level which has not been seen before. The iPhone, with its sleek design and very impressive user friendly features, was able to become one of the world's most successful products. Year after year new sales records were broken. Given the huge demand which exist for smartphones, other companies such as Samsung, Microsoft, Google, etc took advantage of such a high demand and were able to produce for the mass market. As Figure 1 indicates, we have seen an enormous demand for smartphone during the last 7 years:

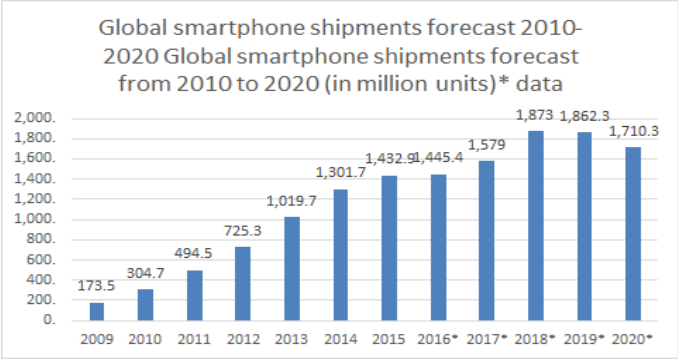


**Figure 1: Number of smartphone shipments from 2009 to 2020 (in million unit)**
Source: https://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/

The popularity of smartphones can be attributed to several factors. First, it could be argued that convenience of smartphone makes it a very desirable device compared to the traditional computing devices such desktop and laptop. Indeed, newer smartphones are quite different than the bulky early devices that were pretty much impossible to carry. Second, the constant network connectivity of smartphones is a huge advantage over traditional computing devices. Through the use of 3G and 4G connectivity, one can not only call and text others using a smartphone, but in addition, can access the Internet through its phone network as well as its wireless network service (Wi-Fi network) whenever such a service is available. Third, partly due to the constant network connectivity, the availability of different application programs designed for smartphone makes achieving many tasks much easier than using the traditional computing devices for both developers and users. In fact accessing information by using different apps is much faster than accessing web sites in order to retrieve valuable information. Lastly, speed of typical new smartphone makes it a very attractive alternative compared to traditional computing devices Desk-Based and Notebook). For these reasons, a large proportion of consumers are switching to Smartphones and Ultramobiles devices. As a result, demand for the traditional PCs is expected to be down while the demand for smaller devices such as smartphones is up.

**Table 1: Worldwide Devices Shipments by Device Type, 2015-2018 (Millions of Units)**

| Device Type | **2015** | **2016*** | **2017*** | **2018*** |
|---|---|---|---|---|
| Traditional PCs (Desk-Based and Notebook) | 246 | 232 | 226 | 219 |
| Ultramobiles (Premium) | 45 | 55 | 74 | 92 |
| **PC Market** | **290** | **287** | **299** | **312** |
| Ultramobiles (Basic and Utility) | 196 | 195 | 196 | 198 |
| **Computing Devices Market** | **486** | **482** | **495** | **510** |
| Regular Phones | 478 | 514 | 404 | 161 |
| Smartphones | 1,432 | 1,445 | 1,579 | 1,873 |
| **Mobile Phones** | **1,910** | **1,959** | **1,983** | **2,034** |
| **Total Devices Market** | **2,396** | **2,441** | **2,478** | **2,545** |

*Expected.
Note: The Ultramobile (Premium) category includes devices such as Microsoft's Windows 8 Intel x86 products and Apple's MacBook Air. The Ultramobile (Basic and Utility Tablets) category includes devices such as, iPad, iPad mini, Samsung Galaxy Tab S 10.5, Nexus 7 and Acer Iconia Tab 8.

Source: Gartner, http://www.gartner.com/newsroom/id/3516317

Further analysis of Table 1 provides important information. Out of 1.91 billion mobile phones about 1.432 billion (close to 75%) are smartphones. Comparing the number of traditional computing devices with the number of smartphones reveals another interesting trend. As Table 1 indicates as early as 2015, the number of smartphones shipments is almost 3 times of number of Pads, Tablets, Netbooks, Notebooks, and Desktops shipments in total. This data indicates that consumers recognize the importance of smartphones and they trade in their traditional PCs and replace them with smartphones. Consequently, the consumer demand for smartphone is expected to increase as the demand for the traditional PCs (desktop and laptops) decreases. This trend is expected to continue in a near future. Now we concentrate our attention on smartphone itself and its market share.

These days, the smartphone market is highly competitive and to some extent is a saturated market. Indeed, several major hardware and software companies are rigorously competing to attain the leading position in their respective areas. For example, when we examine the operating system for smartphones, we observe that close to 99% of the market belongs to only two operating systems (Android and iOS). Google introduced Android in 2007 as an operating system for smartphones. Android is open source and available in over 100 languages. On the other hand iOS is the operating system for iPhones since 2007 when the first iPhone was introduced.

**Table 2: Worldwide Market share based on Operating System**

| **World Wide Market Share based on Operating System** | | | | |
|---|---|---|---|---|
| Period | Android | iOS | Windows Phone | Others |
| 2015 Q4 | 79.60% | 18.70% | 1.20% | 0.50% |
| 2016 Q1 | 83.50% | 15.40% | .80% | .40% |
| 2016 Q23 | 87.60% | 11.70% | .40% | .30% |
| 2016 Q3 | 86.80% | 12.50% | .30% | .40% |

Source: IDC, http://www.idc.com/promo/smartphone-market-share/os;jsessionid=32A8A885761B9BA01C8F080672A388C7

Based on Table 2 Android is the most popular and iOS is the second most popular smartphone-oriented operating systems. Furious competition has continued between these two operating systems for several years. Furthermore, it can be said that as a result of heated competition, Samsung's Hardware, which runs Android as its software has emerged as a major competitor to Apple's products (iOS developer). Thus, for the purpose of this paper, we will examine how these two forces address major ubiquitous security flaws.

In order to accurately compare the security issues of smartphones, it is important to discuss how the two largest smartphone operating systems (iOS and Android) approach security. In particular it is first necessary to discuss how the two units view the interaction between software and hardware. The traditional mantra for technology companies that manufacture computers entails ensuring their systems and products are interchangeable. This way, hardware companies such as Samsung can make products that are not dependent on any one particular software, and software companies such as google can develop programs that are not contingent on anyone particular hardware. On one hand, this separation of powers provides an inherent benefit to both parties as they can focus on creating more specialized products and providing value in different domains. On the other hand, this separation of powers creates environment for possible vulnerabilities since there are so many variations of hardware devices and software programs which can be manipulated by hackers and malicious code developers.

Apple Inc, however does not follow the schema, as its former executive, Steve Jobs firmly believed that an integrated system, in which the hardware and software are tightly linked, would provide Apple with long term stability, and its customers with an optimal user experience.

Thus, it should be quite clear why Android follows an open-source model whereas iOS follows a closed-source model. If a major goal of a company is to attain a financial benefit from the exchange of a product or service, then sourcing models are provide part of the picture of how a software company intends to achieve that goal. In an open source system, such as Android's, the source code is made available publicly for non-commercial use online since their priority is not to sell the software to consumers but to sell the permissions to use their software to hardware companies. It is in Android's best interest to keep all their source code available for developers to improve upon as it will provide more exposure to skilled developers who are willing to contribute to the community. As a result of this policy, during the last 7 years, the number of Android users increased drastically. Further discussion of this policy reveals how Android has become such a dominate force in smartphone operating system. First, since Android is freely available to hardware companies, hundreds of companies have adopted the platform and they were able to develop some amazing smartphones. Second, many users embrace the idea of software versatility and flexibility of Android. Third, since Android is an open source, then many software developers work on developing different application programs so a huge number of application programs are developed for Android based smartphones without effort on the part of parent company (Google).

Apple's scenario, however, is quite different than that of Android's. Since Apple produces a highly integrated products, it is not in their best interest to allow their software to the open-source because through integrating their software and hardware, they have a better control on all aspects of their products so they can bundle them as packages. Obviously, this approach makes Apple in control of all stages of production of its products. Any modification or change must be approved by Apple after rigorous testing.

It can be noted that lately, Samsung and Google have deviated from their original business model and moved toward producing more integrated products. One can conclude that this move is in response to addressing the security vulnerability of their products since an integrated product seems to have less security issues.

## *2. Discussion of Security Flaws of iOS and Android*

In this section we examine several iOS and Android malwares which have caused a great concern among owners of iOS and Android based smartphones. Regarding iOS we discuss three major flaws like Masque Attack, XcodeGhost, wireLuker, and Spyware. For Android we discuss several major flaws such as Spyware, QuadRooter, The 'Certifi-gate"m RST, 'Stagefright' MMS, and Android Installer hijacking.

### 2.1 Masque Attack

It was a flaw in some versions of iOS. FireEye, a cybersecurity company, was able to discover this flaw. In this attack, users of iOS iOS 7.1.1, 7.1.2, 8.0, 8.1 and 8.1.1 beta, and on jailbroken and non-jailbroken devices were fooled to download and install apps that have been deceptively created with the same bundle identifier as an existing legitimate app which is available in app store.

### 2.2 Xcode Ghost

Xcode is software which used to develop apps for iPhones and iPads. XcodeGhost is a malware which infect Xcode by sitting in background of legitimate apps and mines them for data like an invisible person cheating on an exam. When the user launches apps, XcodeGhost starts picking information regarding name of infected app, the app bundle identifier, the device name, etc.

### 2.3 Wire Lurker

It is called "WireLurker" because it monitors any iOS device connected to USB with an infected OS X computer/laptop and installs downloaded third-party applications. It is the first known malware that can infect installed iOS applications similar to a traditional virus. WireLurker exhibits complex code structure, multiple component versions and file hiding.

### 2.4 Spyware

In general, the aim of Spyware is to collect sensitive information about a person, organization, or a device and send it out such information without the user's permission. In Android, the information contains device id, apps info, call and SMS log, contacts, locations, and login and password details can be collected and send out to the third party without users consent. The information could be sent out via Internet or SMS messages. This flaw is common among traditional PCs, Tablets, and smartphones.

### 2.5 Quad Rooter

Quadrooter was discovered in August 2016. It is a set of four vulnerabilities affecting close to 900 million Android smartphones (80% of all Android phones) and tablets that use Qualcomm® chipsets. QuadRooter covers four security issues found on the chipset drivers for Qualcomm LTE modems common to many recent Android handsets. This is actually a hardware issue rather than a software issue. As a result, Qualcomm which provides this chip distributed patch to each maker. However, this patch takes a consider amount of time to implement (since there are many makers which are using this chip).

### 2.6 The 'Certifi-gate' mRST flaw

This is a flaw that was found in several brands of smartphone such as Samsung, LG, HTC, Huawei and ZTE running Android versions up to 5.1. Hackers can sneak a fake app onto a smartphone which exploits the flaw in a way that elevates the hacker's permissions. From that point on, the hacker has complete remote control over the phone.

### 2.7 Stage fright MMS flaw

It is one of the most serious attack on the Android based smartphone. It affected around 95% of all Android users. Hackers could exploit the issue by sending a malicious video message to almost every Android users. This message is executed automatically. Incredibly, no user interaction is needed and the message could become invisible and delete itself.

## *3. Steps to Improve Security of Smartphones*

In this section we intend to provide an overview of security improvements which can be used for Android and iOS smartphone operating system. Security vulnerabilities of smartphones has been the main focus of many research studies lately. Android by far is the most dominated smartphones as Table 2 indicates (86.6% based on the third quarter of 2016). IOS is the second major operating system. As a result in this study we concentrate on major features of these two operating systems and discuss different approaches which are implemented with regards to their security. First, we focus on Android based smartphones and discuss methods to improve Android based smartphones. In particular, we focus on the SEAndroid and containerization in order to improve the security of Android OS. One of the main characteristics of Android applications is running in a sandbox and containerization (an isolated area of the system that does not have access to the rest of the system's resources). The goal of sandboxing is to isolate an application to prevent malware, intruders, system resources or other applications from interacting with the application and any of its sensitive information secured by the container. By using the sandboxing security approach, Android attempts to localize any security issues and prevent it from separating to other sectors. This approach has been successful. For example, Google Chrome browser using a sandbox approach which has made it one of the most secure browsers.

### 3.1Security Enhancement for Android (SEAndroid)

Security Enhanced Android (SEAndroid) is a Linux kernel security module that provides centralized access control policy management for each device. It is a project to identify and address critical gaps in the security of Android. Initially, the project is enabling the use of SELinux in Android in order to limit the damage that can be done by flawed or malicious apps and to enforce separation guarantees between apps. Android uses SELinux to enforce Mandatory Access Control (MAC) over all processes running with root. In Android Open Source Project, it includes SELinux in enforcing mode. In enforcing mode, illegitimate actions are prevented and all attempted violations are logged. Regarding other technical issues, Android is a Linux kernel based mobile operating system. The Linux kernel provides a multi-user nature and discretionary access control (DAC) enforcement module on top of which all Android layers are sitting. Android utilizes the kernel-level sandboxing and isolation mechanism to separate apps from one another, and control the communication between apps or resource accesses. However, Android has some inherent weaknesses associated with DAC in its security model; these can cause vulnerabilities in the system's security. But Securities Enhancements for Android is introduced to mitigate the above shortcomings. Obviously, these enhancements have improved the security of Android based devices; however there are still some security vulnerabilities. Below are some important security features which became available as a result of Securities Enhancement for Android.

**Application verification** - Different application programs are verified and they are screened by an application verifier before they are able to be installed. App verification can alert the user if they are about to install an app that might be harmful. Indeed, if the app is a dangerous one, its installation can be blocked.

**Always-on VPN** - Virtual Private Network (VPN) can be set so that applications will have access to the VPN network only after the VPN connection is established. This prevents applications from sending data across other networks.

**Device Monitoring Warnings.** Android users can receive warning if a certificate has been added to the device certificate store which is capable of monitoring of encrypted network.

**Encrypted by default.** Android devices out-of-the-box has full disk encryption and can be enabled by default in order to improve protection of data on lost or stolen devices.

**Smart Lock.** Android provides flexibility for unlocking devices. It can allow devices to be unlocked automatically when closed to another trusted device (via NFC, Bluetooth).

**Fingerprints**. Recently, many computing devices are equipped to different biometric measures in order to control access. Smartphones are using low cost measures such as fingerprint scanners to unlock with just a touch. In addition, in many smartphones, fingerprints can be used to lock and unlock encryption keys. Android based smartphones are equipped with this technology. It is a hope that this technology be able to make it impossible for other individuals to use the smartphone without the owner's consent. However, this method has very false positive/negative result for now and is far from perfect.

**File-based Encryption**. Encrypting is used at the file level, instead of encrypting the entire storage area as a single unit. This will better isolate and protect individual users and profiles on a device.These steps obviously have helped Android to deal with many security threats. However, even after these steps, Android still remains vulnerable. In the next section we will discuss a few security flaws of Android and iOS operating systems.

### 3.2 Sandboxing, Containerization, and Air Watch

Sandboxing is an efficient way to minimize the effect of malicious code and other security threat by trying to localize and contain its effect. On the other hand, containerization is the method of securing a device for corporate use by putting a part of it behind some type of authentication. A secure data container is a third-party mobile application that is used to separate and secure a portion of device's storage from the rest of the device. The objective of sandboxing is to isolate an application to prevent malware, intruders, system resources or other applications from interacting with the application and any of its sensitive information secured by the container.

However, it must be understood that sandboxing can't protect everything. The sandboxing approach is available on almost all smartphones operating systems such as android, iOS, Blackberry and Windows phone while containerization is mainly employed by Android based smartphone. It is worth noting that iOS is using AirWatch in order to manage employee access, security and privacy concerns.

### 3.3 Security Enhancement for iOS

Apple is the provider of iOS operating systems which support devices like iPhone, iPad, iPod. When it comes to security, everyone who is in IT or a non-IT field should be feeling pretty good about the iOS operating system. The following are measures that Apple is talking to provide a safe and comfortable service to its consumers.

- Password protection is added to Mail, Calendar, Contact, Message, and third party apps. ·
- Individual email encryption is supported through the use of Secure/Multipurpose Internet Mail Extensions technology.
- Users can authenticate to enterprise apps without having to re-enter their credentials each time they switch between apps.
- Device's name can be set remotely. Also remotely disable and wipe or restore features when necessary.
- Apple is now able to block Wire Lurker by blocking enterprise certificate that it was using to install malicious apps.
- To avoid being compromised by Masque Attack, only install apps that come directly from the App Store, don't click on Install if you see a pop-up on a website or if you see a prompt to install an update to an app like Flappy Bird. Also, if iOS displays an alert that an app is from an Untrusted App Developer tap Don't Trust and uninstall it.

## *4. Conclusion*

In conclusion, as the number of smartphones is expected to increase so does the number of malware attacks and security threats. Smartphone developers are attempting to encounter these threats by introducing new measures. It can be said that these measures at best are partially successful. Indeed, we have observed uprising trends in the number of malware attacks especially attacks that target Android based operating systems during the last several years. As we keep finding solutions for these attacks, new attacks will get smarter and aim to generate more damages. In Android OS, it is tougher to create walls against such attacks, because of its open source system. Even SEAndroid, sandboxing, and containerization, the most protective concepts for Android OS, have relatively limited effect in order to keep smartphones totally safe from such malware attacks and data vulnerabilities. Furthermore, we expect the continuing increase of smarter Android malware in the future, which effectively takes advantage of social engineering and bypass these security enhancements. Overall, iOS seems to be relatively safer since it is based on an integrated system. Consequently, in iOS very few steps need to know and implement in order to keep device relatively safe from third party intruders. Also, the existence of iCloud storage makes it easier to protect applications and information. Despite all these positive points, iOS is still vulnerable. In conclusion it can be said that no OS is quite safe.

## *References*

Brook, Chris. "Backdoor Found in Firmware of Some Android Devices." *Backdoor Found in Firmware of Some Android Devices*. Threat Post, 21 Nov. 2016. Web. 2017.

Chau, Melissa. "Smartphone OS Market Share, 2016 Q3." *IDC Analyze and Future*. N.p., n.d. Web. 21 Jan. 2017.

Dunn, John E. "Android's 6 Biggest Security Flaws 2016." *Techworld*. N.p., 09 Aug. 2016. Web. 26 Jan. 2017.

Epstein, Zach. "Android's Biggest Strength Is Driving People to the IPhone." *Yahoo!* Yahoo!, 20 Jan. 2017. Web. 21 Jan. 2017.

Froehlich, Andrew. "InformationWeek News Connects The Business Technology Community." *InformationWeek*. N.p., 10 Mar. 2015. Web. 26 Jan. 2017.

"Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016." *Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016.* Gartner Press Release, 19 May 2016. Web. 23 Jan. 2017.

Hildenbrand, Jerry. "Google Creates Android Security Updates Google Group for More Transparency." N.p., 13 Aug. 2015. Web. 22 Jan. 2017.

Stilgherrian."Android, You Have Serious Security Problems." *ZDNet*. ZDNet, 04 Dec. 2015. Web. 26 Jan. 2017.

Woods, Viveca. "Worldwide Device Shipments to Grow 1.9 Percent in 2016, While End-User Spending to Decline for the First Time." *Worldwide Device Shipments to Grow 1.9 Percent in 2016, While End-User Spending to Decline for the First Time*. N.p., 20 Jan. 2016. Web. 21 Jan. 2017.