International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.13-26
http://dx.doi.org/10.14257/ijsia.2016.10.2.02

Security Threats on Mobile Devices and their Effects: Estimations for the Future

Murat Yesilyurt[1*], Yildiray Yalman[1]

[1]*Computer Engineering Department, Turgut Ozal University, Ankara, Turkey*
{myesilyurt, yyalman}@turgutozal.edu.tr

Abstract

Portable devices are today used in all areas of life thanks to their ease of use as well as their applications with unique features. The increase in the number of users, however, also leads to an increase in security threats. This study examines the threats to mobile operating systems. Addressing the four mobile operating systems (Android, Apple OS (iOS), Symbian and Java ME) with the highest number of users, the study provides statistical information about the features of the corresponding operating systems and their areas of use. In the study, the most important threats faced by the mobile operating systems (Malware, Vulnerabilities, Attacks) and the risks posed by these threats were analyzed in chronological order and the future-oriented security perspective was suggested..

Keywords*: Vulnerabilities, Threats, Attacks, Mobile Devices, Mobile Operating System*

1. Introduction

The internet, used by ourselves in all areas of our daily lives, has shown a great improvement in recent years. Accordingly, the devices to connect this virtual environment have undergone a great change and the use of mobile devices has quite increased. Almost all communication and processes can be carried out through the mobile tools (documents, social network, online shopping *etc*.) facilitating the daily life. The increase in this number, however, brings along some security problems.

The unknown Wi-Fi settings, accepting all unidentified applications, connecting to untrusted sites and downloading applications from such sites can be listed as the major ones of these problems. It is of great importance that certain safety precautions should be taken for the mobile tools in which private information and documents of the users are stored. This study examines the operating systems of the most-preferred mobile tools and the threats towards these operating systems and provides detailed information about them.

Chapter 2 discusses in detail the mobile operating systems that are, currently, most widely used. The Chapter 3 focuses on the threats to mobile operating systems and their functions and analyses the types of these malicious software, vulnerabilities and the attacks made. Chapter 4, however, examines the future status of mobile OSs based on their security levels.

2. Mobile Operating Systems Versus Computer Operating Systems

Operating systems (OS) are the software-based interfaces necessary for users to manage, use and operate the hardware units. Figure 1 shows the common structure of an operating system. If the hardware to be managed is portable device such as Smart Phone, Tablet PC, PDA *etc*., the operating systems of such devices developed to enable these devices to run as a personal computer are also called Mobile Operating System (Mobile OS).

ISSN: 1738-9976 IJSIA

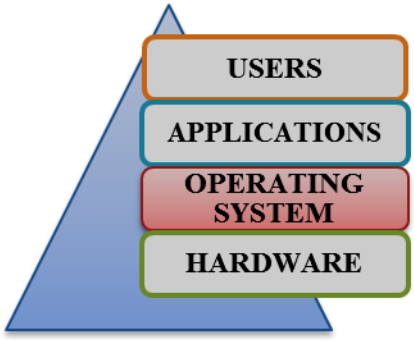


Figure 1. Operating System Common Structure

The number of mobile devices is increasing day by day thanks to their portability, ease of use and the increase in their features with the advancing technology. With this increase, great development and changes have occurred in the operating system preparing the ground for meeting the demands of users. Figure 2 shows the usage rates of personal computer operating systems and mobile OSs by years.

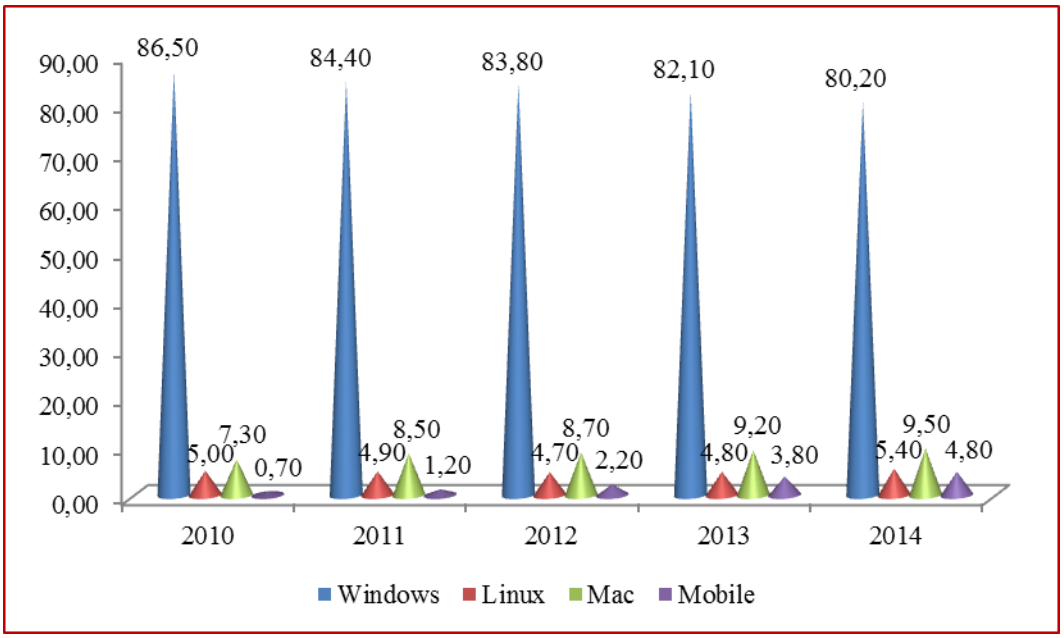


Figure 2. Usage Rates of all Operating Systems by Years [1]

Figure 3 shows the usage rates of the operating systems used between 2010 and 2014. The values shown in the figure are the values obtained at the end of each year. For example; while Mobile OS usage is 3.80 % at the end of 2013, this rate increases to 4.80 % at the end of 2014. Among the operating systems used for personal or corporate purposes, the significant advantage of Windows draws attention. However, it is observed that the mobile OSs are increasingly being used more and even, considering the first three months of 2015, its usage rate increases to 5 % [1, 2].

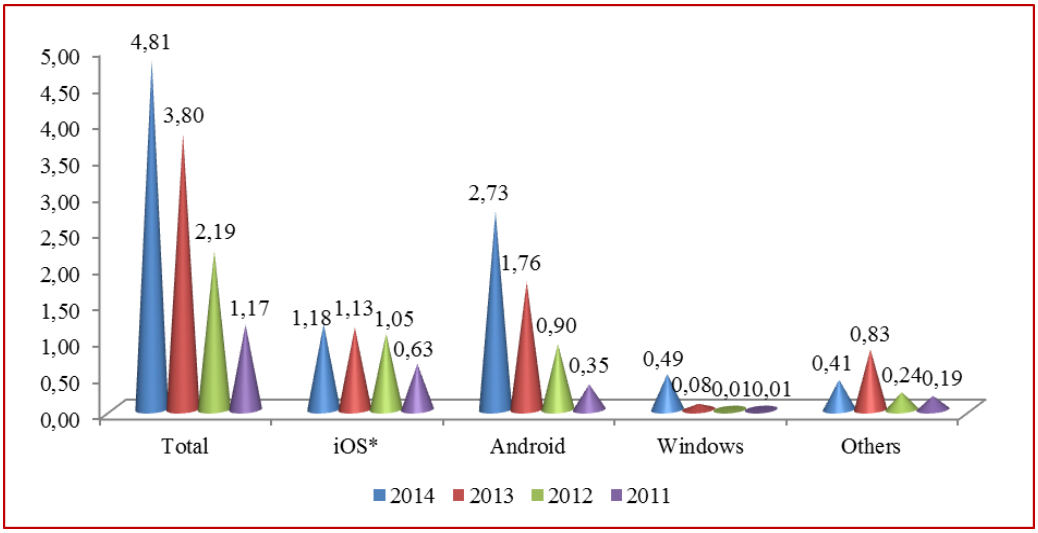


Figure 3. Mobile OS Usage Averages by Years [2]

Figure 4 shows the market analysis dated March 2015 (Market Share Statistics for Internet Technologies) of all mobile operating systems in use today. Accordingly; while Android OS, one of the mobile OSs, is the most widely used mobile OS with a rate of 47.51%, it is followed by iOS with a rate of 41.97%. It is seen that the other mobile operating systems Java ME (3.49%), Symbian (3.31%) and Windows phone (2.57%) ranks as, respectively, the third, fourth and fifth. There are other mobile OSs which are not included in this chart but in use (Black Berry, Samsung, *etc*.). However, their usage rates are lower than the others [3]. This study analyses iOS and Android operating systems which constitute the two most widely used operating systems.

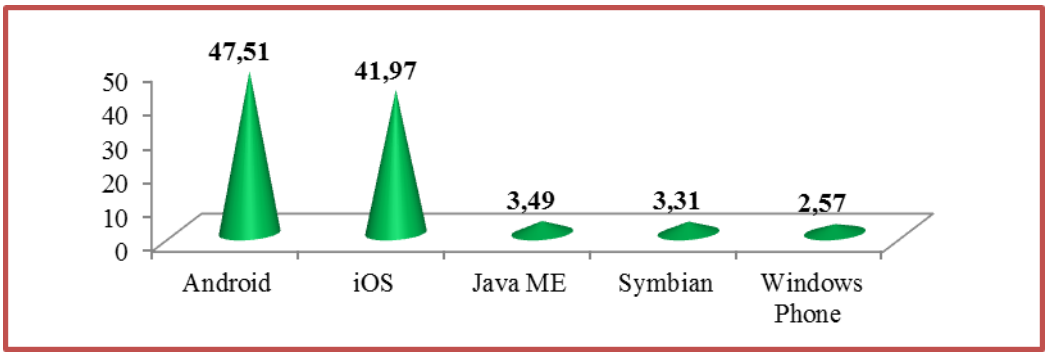


Figure 4. Mobile OS Market Share Ratios Including the First Three Monthsof 2015 [01]

2.1. Android Mobile OS

As an open-source code operating system, Android is a Linux-based mobile OS and is developed by Google. Android uses Linux version 2.6 for the core system services such as security, memory management, process management, network stack and driver model [4]. In addition, it serves as abstraction layer between the core, hardware and software stack created using the C programming language and other layers.

Abstraction layer includes timing and libraries. The timing contains the core libraries providing functionality in the basic libraries created using the Java programming language. These libraries work according to their functions in a virtual machine (Dalvik Virtual Machine) for each Android application [5]. It offers a wide, rich and innovative opportunity to the developers for top-level applications used by various components of

the Android system such as Libraries, Media Libraries and 3D libraries. Moreover, Android offers a wide variety of free and available features such as device hardware, access location information, constantly running background services, timing warning systems and adding notifications to the status bar. All applications are written using the Java programming language [6].

2.2. Apple Mobile OS

First developed in 2007 by Steve Jobs, the founder of Apple, iOS is a mobile operating system used only in Apple-branded products (iPhone, iPod, iPad) for now [7]. In analogy with the other operating systems, iOS architecture is built on four platforms integrated with each other [8]. The first platform, Cocoa Touch, provides the basic infrastructure used by the applications. For example; it constitutes the layer written using C language providing an object-oriented support for file management, network operations and more. This layer includes Map Kit, iAD, Game Kit, Events (Touch), View Controllers and UIKit. The Media Layer constitutes the section that enables using Audio, Animation video and Image formats (JPEG, PNG, TIFF) and documents. Core Services (Core OS) - the third layer-, Core operating system and the core service layers contain iPhone OS-specific basic interfaces for low-level data types, startup services, network connection and accesses. These interfaces are usually C-based and core-centered and they offer technologies involving SQLite and POSIX threads as well as access to UNIX sockets. The Media Layer which constitutes the last layer of Apple iOS, however, contains the basic technologies used for 2D and 3D drawings and audio and video support. This layer contains C-based technologies such as OpenGL ES, Quarts and Core Audio. In addition, there is an Objective-C based animation engine and a core Animation application in this layer.

In addition to all these features, Apple Cloud Computing allows direct installation of all information and documents thanks to its iCloud system allowing data storage and in the context of mobile application development, Apple's iCloud system (2013 Apple Inc.) explores the limitations that may occur [9].

2.3. Java ME

Java Platform Micro Edition (JavaME or formerly J2ME) operating system was designed by Sun Microsystems for mobile and embedded devices (Blu-RayDisc Players, Printers, *etc*.) and its usage areas has significantly increased thanks to its flexible structure [10]. It consists of seven layers including Java ME system "Application Layer", "Configuration Layer" which contains very specific APIs and has java language virtual machine features and minimum class libraries, "Profile Layer" which supports high-level services and is built on the configuration layer, “Optional Packages Layer” which involves functions or specific applications independent from Profile or Configuration (*i.e*., Java APIs for Bluetooth, Location APIs for J2me, J2ME Web Services), Vendor specific classes, Native Operating System and Hardware. In addition to its flexible user interfaces, its rich and robust security in terms of functionality and its support for network and offline applications, Java ME is also designed in a way to be used on many portable devices and to improve the performance of the device used.

2.4. Symbian

Symbian is a mobile operating system using open source code. Symbian which is an open source software written using the C ++ programming language, was first developed in 1977. It had become very popular until the end of 2010. After this date, its place was largely taken by Android [11].

Symbian is composed of layers such as OS Libraries, application Engines, KVM, Servers, symbian OS Base-Kernel and Hardware. Being used for many portable devices

from the date it was developed until 2010, Symbian is also known as a software with an outstanding security among the mobile OSs.

2.5 Windows Phone

It is an operating system developed by Microsoft for smart devices. This 32-bit Windows CE 5.0-based mobile operating system which was first developed for PDAs is now used by the Smart Phones and touch devices. In 2003, it was named as Windows Mobile. Windows Mobile experienced a drop against its rivals by the end of 2010 and Microsoft has gradually renovated this operating system by a decision taken and put it on the market as Windows Phone [12].

As it started using the .Net Compact Framework structure, Windows Phone has had many features and advantages. For example, its coding language is able to integrate the written applications into mobile devices thanks to its independent compilation structure (Common Language Runtime -CLR). Windows Phone is moving towards becoming a promising operating system thanks to the special libraries, enhanced device protection and software security features of .Net Framework oriented for developing mobile applications [13].

Table 1 shows the comparison of some features of mobile operating systems. It is seen from the table that the majority of the software used are open source software. Another important point is that none of these mobile operating systems, except for Apple and Windows, produce mobile device and that, the OS-based structure is only different in Apple and Microsoft.

Table 1. Comparison of the Mobile Operation Systems

Android	iOS	Windows Phone	Symbian	Java ME
Open Source Code	Closed Source Code	Closed Source Code	Open Source Code	Open Source Code
Application Download: Google App store or Free	Application Download: Apple Store	Application Download: Windows Phone Store	Application Download: Nokia Symbian or Free	Application Download: Free
User Defined Reorganization	No User Defined Reorganization	No User Defined Reorganization	User Defined Reorganization	User Defined Reorganization
Mobile Device is not special to Google	Mobile Device is special to Apple	Mobile Device is not special to Microsoft	Mobile Device is not special to Symbian Foundation or Nokia	Mobile Device is not special to Sun Microsystem
OS Based: Linux	OS Based: Darwin	OS Based: WindowsNT	OS Based: Linux	OS Based: Linux
No Device independent system updates	No Device independent system updates	No Device independent system updates	No Device independent system updates	No Device independent system updates
Access to external storage: YES	Access to external storage: NO	Access to external storage: YES	Access to external storage: YES	Access to external storage: YES

3. Threats of Mobiles Operating System

As all devices with a internet connection, there are also a wide variety of threats to the smart devices using mobile operating system. In line with the portable devices, the malicious software industry is also growing both in technological and structural terms. These threats are discussed in three main categories including Malware, Vulnerabilities and Attacks (Figure 5).

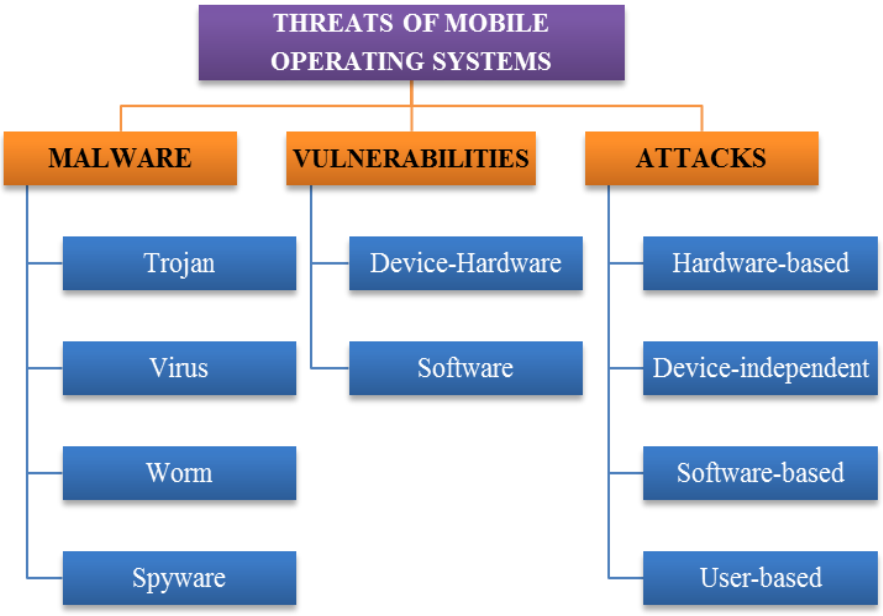


Figure 5. Threats of Mobile Operating Systems

3.1. Malware

Malicious Software (Malware) are, in its simplest expression, the malicious software aimed at private specific information which disturb users, may cause breakdown of the device and lead to results such as causing information and documents belonging to the user to be stolen or become unusable [14]. These illegal software which are not installed by the user are used for all attacks from the outside taking advantage of the vulnerabilities in the device or system. The major ones of these software are Trojans, Worms, Virus and Spyware. The first known malware is Cabir which was created for the Symbian operating system in 2004. Cabir is a malicious software which infected the Nokia 60 series and affected many smartphones. This worm writes the word "Cabire" on the screen of the phone infected and uses Bluetooth connection to spread itself [15]. Apple is more protected against OS malware software thanks to its closed system. The OS which becomes the target of Malware attacks most is Android OS. The biggest reason for this is that the applications can be obtained from many secure-insecure sources.

- Trojans: The main purpose of Trojan software is not to spread themselves but to seize the device management and information. With this aspect, they differ from the worms and viruses. The most widely used spyware are, in this respect, the keyloggers. The purpose of these software transmitted under the cover of another file and unintendedly activated by the user is to get the device entirely under control in the background. These malware are generally carried inside a more innocent software and not noticed by the user. For this reason, while downloading an application necessary for the smart devices, it is of utmost importance to use checked and reliable software. However, this is a little harder for the Android devices. Because, those who use such devices are also able to download applications from elsewhere other than the Google App Store. And even, since they can

recognize the external units such as USB or SDcard, the Trojans can also get into the devices through such devices and create a vulnerability in the system. This is a bit more difficult for iOS compared to the Android devices. Because Apple Store constitutes the only option to download application [16].

- Virus: These are the malicious software which have some features such as penetrating into the existing documents and sending them elsewhere, distorting their contents and making them unusable and slowing down the hardware elements. For the spread of viruses, infected programs should also be installed in other devices. In other words, the infected program must also be sent to other devices by the user. For example; in 2010, the "Zombie" virus infected more than 1 million smartphones in China and caused a loss amounting to $300,000 per day. Besides its numerous damages, it also leads to data loss, data leakage and even disruption of the conversation [17].

- Worm: Worms which are counted among the malware contain harmful and misleading instructions. The worms affecting mobile devices do not require user interaction in order to be effective and are usually transmitted through the text messages (SMS) or picture messages (MMS). Worm is actually a kind of virus. However, it does not require user interaction to reproduce itself. For example, clicking on a file or opening a plug-in sent by e-mail activates the worm. A security vulnerability in the operating system would be sufficient for Worm infection. The Worm penetrates using this vulnerability and integrates itself into a service running in the operating system. After this stage; it can act as a spy inside the device, send the required information to the center managing itself, cause clogging and slowing down in the Internet bandwidth through creating an unnecessary data flow and degrade the performance of the device.

- Spyware: Spyware software are used to collect information on a specific subject. Though specifying that they are used for advertising and promotional purposes (adware) or to provide better service to users (cookies), these software collect information about a person or organization and send those information to someone else without their consent. In this sense, it works like a Trojan and can be used by malicious people. It is also a software aimed at taking control of the devices infected.

In the studies performed by security firms, it is seen that malware software are not only used by hackers but also created by the profit-oriented "teams" making cooperation in this regard. For example; in an incident in 2013, the Trojan 'botnet Trojan-SMS.AndroidOS.Opfake.a' enabled the spread of the malware software 'Backdoor.AndroidOS.Obad.a' through sending a spam containing the malware to its victim list [18]. Figure 6 shows the top malware categories of published by CISCO. Trojan software are seen at the highest level among the malware software with a high rate of 64 %. [19].

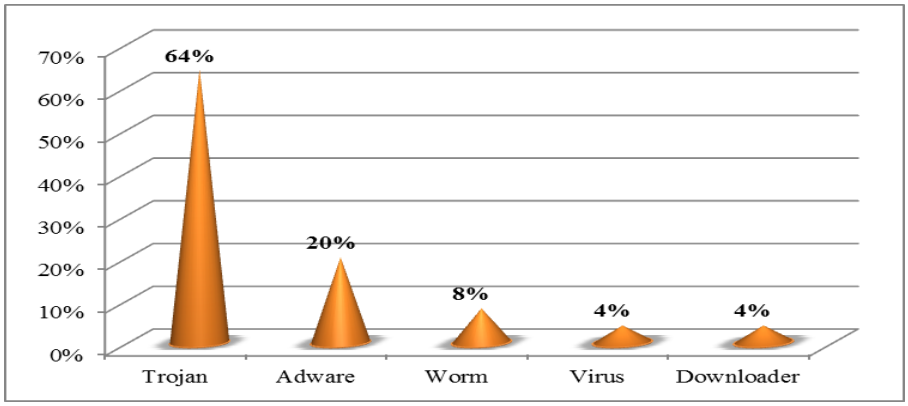


Figure 6. Rates of Malware Software Affecting Mobile OSs [19]

3.2. Vulnerabilities

The weaknesses occurring in the system security procedures, internal controls, design and applications are among the security vulnerabilities in the device. These vulnerabilities can be grouped under several headings. In the present study, the analyze is carried out in two main categories including device-hardware vulnerabilities and mobile operating system and application (software) vulnerabilities:

3.2.1. Device-Hardware Vulnerabilities

The most-encountered problem which should be considered first in this regard is the agedness of the device. Because, the manufacturers do not support the devices manufactured before a certain date. Therefore, the device may not receive security updates.

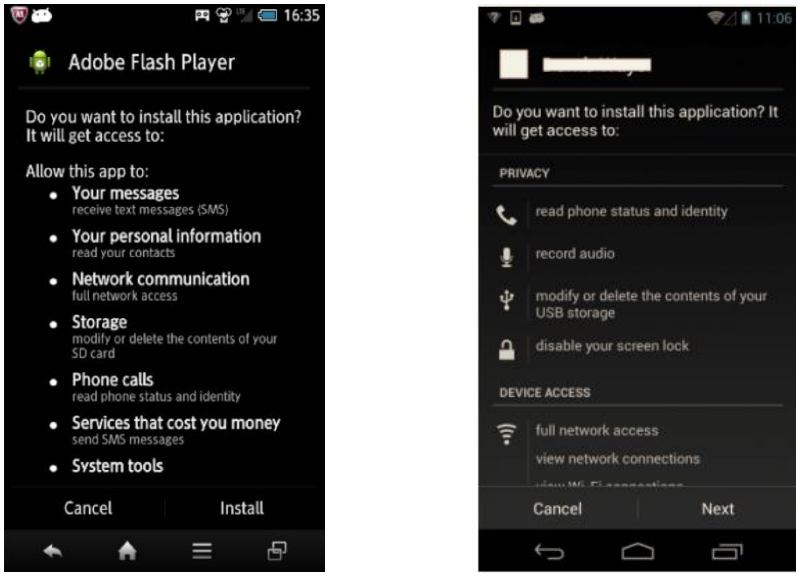
The second issue, however, is the inability of the mobile devices in assuring the safety of the ports they use while connecting to a network or the Internet. The fact that the mobile devices have generally no "navigation" limit used in the Internet environment and there is no firewall to control this is an important vulnerability. A hacker can easily access to the mobile devices via this unsecure port. In such cases, the software called "firewall" which protect these ports must be used. Thus, the user will be asked for a permission while connecting to the mobile device and will be able to see it. There may be unauthorized changes ("jailbreaking" or " rooting") on the mobile devices which are not using a firewall. Jailbreaking which provides an escape for Apple iOS is the method applied to obtain an application that does not belong to Apple (iTunes, App store.) or cannot be downloaded due to some restrictions from any other source. This method allows to have access to the operating system of the mobile device and this constitutes a vulnerability. In addition, the "jailbroken" devices may not receive security updates of the manufacturer and the devices without the necessary updates may become vulnerable to threats [20].

3.2.2. Software Vulnerabilities: The out-datedness of the mobile operating system is also an important vulnerability. Yet, the best known of the security vulnerabilities arising from software is the use of an old Mobile OS and out-datedness. For example, an Android supports application installation from Google Play or another file system. Since Google file system is a protected area, the downloads or packages (APKs) from this area are secure. However, downloading APK files from third-party application stores, mobile ad libraries and local storage units (*i.e.*, sdcard) is often unprotected. Such vulnerabilities are tried to be met by the firms through new versions or patches.

The shared open source common components also constitute an important vulnerability. Another vulnerability occurring in all open source software is in the design of the system containing common open source components such as WebKit and Linux kernel. These components have a reusable structure in order to reduce the costs and this is a common practice in large open source systems such as Android. A vulnerability has been discovered in WebKit or Linux, however, a patch was released in order to use in solving this problem. Apple's iPhone-like WebKit and BSD kernel derivative (Darwin) constitutes the common software components. The problem at this point is not its re-use but where it is employed. In this regard, Android has put the patch model into practice with a little delay [21].

The vulnerabilities occurring during the installation of APK files are very common. The presence of a vulnerability known as "Check Time" of the package installer has also been identified. This means that it is replaced by an open APK file or can be changed during installation without the user's knowledge. This open package constitutes the vulnerability of the installer and affects APK files downloaded from unprotected local storage units [22].

As shown in Figures 7, the vulnerabilities largely arise from the permissions given during the installation of an application. Figure 7-(a) shows the permissions required during the installation of an application downloaded from the Google Play to the Android operating system [23]. All these permissions leave the device wide open to the malware. Users should bear in mind that all permission given can be used by the malware. Figure 7-(b) shows the permission display of an APK application. The system first start the installation process of the APK file through the Package Installer and gets critical information such as application name, application icon, application requests and security permissions. When the user intends to install the application, he/she verifies his/her authorization through these permissions and this is called "Time to Check". In all Android applications; the user selects "Next" to continue with the user setup process following this step.



(a) (b)

Figure 7. Some Required Permissions for a Mobile Application Downloaded from Google Play Store (a) and an APK file (b)

When the user gives such permissions, a vulnerability occurs in the background and the allowed package is replaced by a malware package. Following this process, once the user clicks the "Install" button (“Time of Use"), the Package Installer which will install the APK file installs a different application instead of the set allowed.

In the report released by Symantec; while the number of vulnerabilities affecting the mobile operating system was 315 in 2011, this number increased to 416 in 2012. However, this number declined to 132 with a decrease of 68 % in 2013. It is seen that the number of vulnerabilities in the mobile tools has significantly decreased in 2013 [24]. The major reason for this decline is that the companies (especially Android-Google) developing mobile OSs have eliminated such vulnerabilities through the patches developed by themselves. At the same time, releasing updates at regular intervals for the mobile OSs is the most important factor in maintaining security even against the newly-released malware.

3.3. Attacks

Attacks are the interferences made from outside using a variety of vulnerabilities. This interference are all considered as an attack regardless of whether they are made through malware software or they use vulnerabilities in the smart device or mobile operating system. However, the terms "attack" is generally defines as the attacks made by the hackers for obtaining users' private information without their knowledge.

The first real attack against smartphones was first made by two researchers called Vincenzo Iozzo and Ralf Philipp Weinmann in March of 2010 in order to steal a database from a phone via SMS. This attack was made by looking at an error in the Safari Browser of iPhone 3GS phones and it was aimed to upload the file sent by SMS to the server [25].

In November 2010, however, an attack was directed to the browser in the Android operating system using a common vulnerability [26]. More recently, the first "over-the-air" attack for GSM software which will lead to memory corruption has been introduced again by Weinmann [27]. Moreover, Oberheide and Lanier has identified several different attack vectors for the iTunes App Store [28].

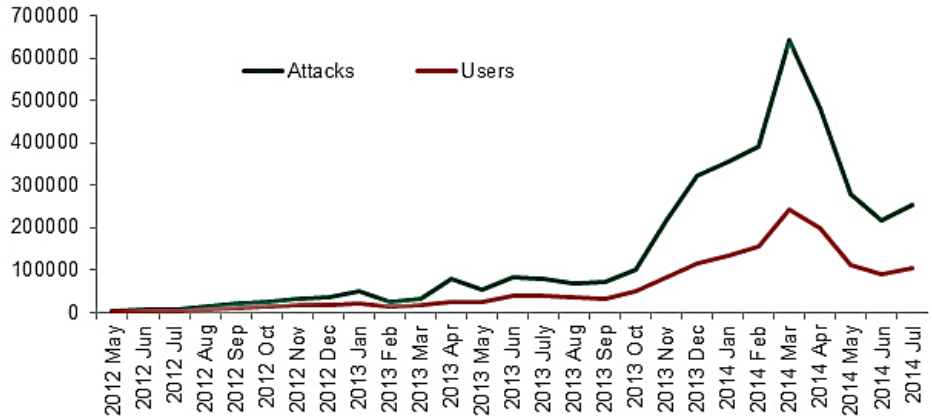


Figure 8. The Relationship Between The Number Of Mobile Device Users And The Number Of The Attacks Between The 2nd Quarter Of 2012 And 3rd Quarter of 2014 [29]

Figure 8 shows the relationship between the number of mobile device users and the number of the attacks between the 2nd quarter of 2012 and 3rd quarter of 2014. Accordingly, it is seen that the number of attacks hits the top in March and April of 2014, however, and then starts to decline [29].

There are various classifications in terms of attacks. One of them is the classification made by Becher which groups the attacks towards mobile devices in four main categories. Hardware-based, device-independent, software-based, and user-based attacks [30].

-Hardware-based attacks: With a broad perspective, hardware-based attacks constitute an element of mobile security. Even if the Mobile Device has any vulnerability, it cannot easily reach to the user information, however, there is an access to the device.

-Device-independent attacks: These are the attacks independent from the device which directly target the mobile device user. They intend to violate the privacy of the user's personal data through wireless connection or wiretapping.

-Software-based attacks: An important part of the technical vulnerabilities on mobile devices are the software-based attacks. Especially the increase in the number of mobile web browser has led to an increase in the vulnerabilities used in this field.

-User-based attacks: Such attacks are not technical attacks. These constitute the attacks made through cheating without using malicious software which are direct to the

mobile device users. These attacks made through "social engineering" and aimed at reaching to private information are today quite common [8]. A large number of the attacks are not technical-based. For example; the Denial of Service (DoS) attacks are not directed through applications or malware installed in smartphones but using the vulnerabilities created by the malformed text messages [31].

In addition to these attack vectors, there are also other types of attacks. However, the aim of all attacks are essentially to find the victim's vulnerabilities and to make attack using a well-intended process and application.

-JTAG (Joint Test Action Group) Attacks: JTAG is the best-known hardware and debug standard. Even though it provides a high control and observability, it also creates vulnerabilities because of allowing for the control of the device at a deep level [32].

-Forensic Analysis: This is an attack vector targeting the privacy of the data stored on the mobile devices. This vector applies to the cases where the attacker has physical access to the device. The attacker takes the device of the user who do not realize this situation under his/her control for a certain time. In such a case, the attacker can reach to the information stored in the device. The second possibility is, however, to obtain the confidential corporate data and personal conversations and today, some studies show that this is the most commonly used method [33, 34].

-Phishing Attacks: This is a kind of attack formed by combining the words "Password" and "Fishing". Phishing in the mobile applications is a threat related to the successful attacks reported. This is an OS-independent method and can be used for all types of devices. Such attacks are made through directing the user to the imitation websites instead of the legitimate ones in order to steal their private information such as credentials, credit card information, user name or password. There are some varieties of this attack such as Similarity attack, Forwarding attack, Background attack and Notification attack [35].

-QR Code Based Attacks: This is an application which has become very popular recently thanks to its large storage capacity due to the QR (Quick Response) code, ease of production and distribution and the fast readability features. However, users usually are not able to understand the type of knowledge contained in it while scanning QR codes content of which are easily encoded. And this provides a suitable environment to direct users to malicious URLs. Google Safe Browsing API and Phishtank API increases the speed in detecting phishing and malware attacks as well as malicious URLs (SafeQR) [36].

-SSL Proxy Attacks: Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption used in many applications today (especially in internet banking) is a protocol that generally reassures users and provides data security. SSL is an encryption scheme and provides adequate security when implemented correctly. Otherwise, applications may be encountered with security threats and unintended vulnerabilities occurs. If this code is left unreviewed, the settings can be changed in an undesired manner and the information which were presumed to be safe and transmitted can be stolen through communication path [37].

4. Estimates for the Future

As the number and usage rates of the open source Mobile OS, the number of malware is seen to show a substantial increase in parallel with them.

Android is a mobile OS that has a quite large area and number of use. However, the number of security problems is also high. Even though Google has actually taken serious steps on security with the patches and updates released by the latter, it is seen in the reports released by the security firms such as Kaspersky and F-Secure as well as in Figure 9, that the malware software are still mostly (98.05 %) send over devices using this operating system. The biggest reason for this arises from the open-source code

application. Despite all its advantages, open source code contains lots of problems in security terms.

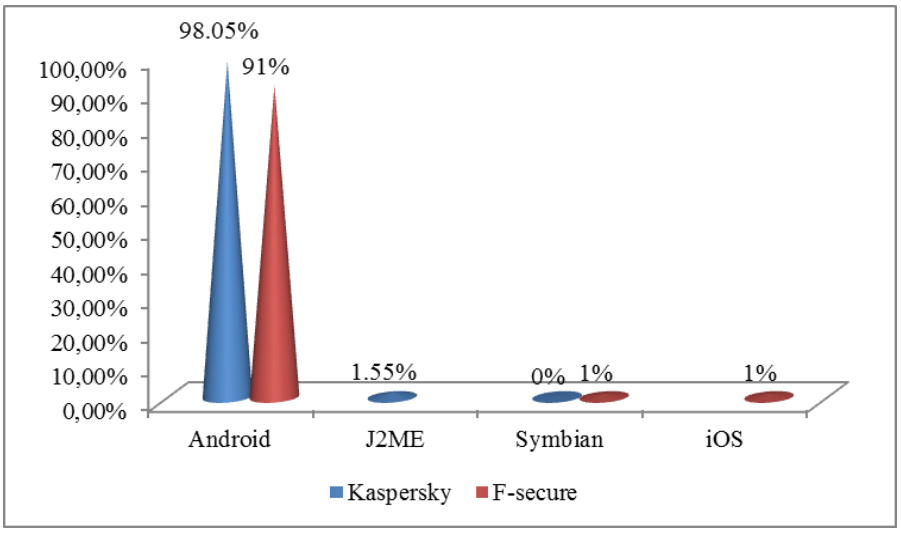


Figure 9. Malware Attacks on Mobil OS [29, 38]

It is certain that the security will become the most important factor in the communication in the future. For this reason, considering the operation and information security, the software like IOS are expected to find a significant place. Apple iOS offers many advantages in terms of security thanks to its closed-code structure. Although its users are restricted within the area of application, it is understood that it will be a preferred OS in the future since it has a better performance compared to the Android and is a less problematic system. Windows Phone, another closed system, is also expected to show the same success it shown in personal computers with Windows also in the portable devices in the future. At least, it is known that they endeavor a great effort in order to emphasize the security. Although it doesn't have an open source code and blocks this development to a certain degree, the increase to be realized by it in the security level will provide a significant advantage in the future. As a language, Java is an effective and rapid language forming the basis of the Android and used for many portable devices. A great effort is given with J2ME in order to become an individual Mobile OS and a certain success is achieved in this regard. However, a new open source OS should meet a great number of requirements in terms of security. In this regard, it is not predicted to be as successful as IOS. Is it better to become the most-widely used operating system or the most reliable OS? This is the most important question that will determine the future.

References

[1] Operating System Browsers, http://www.w3schools.com/browsers/browsers_os.asp, Last Accessed 23 March 2015
[2] Mobile Browsers, http://www.w3schools.com/browsers/browsers_mobile.asp, Last Accessed 23 March 2015
[3] Mobile Operating System Market Share, https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1, Last Accessed 01 April 2015
[4] L. K. Yan and H. Yin, "Droid Scope: Seamlessly Reconstructing the OS and Dalvik Semantic Views for Dynamic Android Malware Analysis", InUSENIX Security Symposium, **(2012)**, pp. 569-584.
[5] Google, "What is Android", http://developer.android.com/guide/basics/what-is-android.html, Last accessed 15 April 2015.
[6] B. A. Yaseen and M. A. Tariq, "Technical Comparison Between Android And IOS With Respect to Their Architecture", Technical Report Documentation Page, Punjab University College of Information Technology, University (PUCIT), Report No:BCSF09A, **(2012)**, pp.1-16.
[7] What is IOS, https://www.apple.com/ios/what-is/, Last accessed 20 April 2015.

[8] M. P. V. Kanoi and Y. Jdiet, "Internal Structure of IOS and Building Tools for IOS Apps". International Journal Of Computer Science And Applications, vol.6, no.2, **(2013)**, pp.220-225.
[9] M. Christian, "Integrating Cloud Computing and Mobile Applications: A Comparative Study Based on Icloud and Sanscode", Journal of Cloud Computing, **(2014)**, pp.1-9.
[10] [What is J2ME, https://www.java.com/en/download/faq/whatis_j2me.xml, Last accessed 21 April 2015.
[11] S. P. Hall and E. Anderson, "Operating Systems for Mobile Computing", Consortium Computing Sciences in College: Rocky Mountain Conference, **(2009)**, pp. 64-71.
[12] Windows CE, https://msdn.microsoft.com/en-us/library/ms905511.aspx, Last accessed 21 April 2015.
[13] T. M. Grønli, J. Hansen and G. Ghinea, "Android vs Windows Mobile vs Java ME: a comparative study of mobile development environments". In Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments, **(2010)**, pp. 45.
[14] A. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. "A survey of mobile malware in the wild", In Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), **(2011)**, pp. 3-14.
[15] A. Axelle, "The Evolution of Mobile Malware", Computer Fraud & Security vol. 2014, no. 8, pp. 18–20
[16] L. Qing and C. Greg, "Mobile Security: A Look Ahead", IEEE Computer and Reliability Societies, **(2013)**, pp. 78-81.
[17] C. Gao, and J. Liu, "Modeling and restraining mobile virus propagation", IEEE Transactions on Mobile Computing, vol.12, no.3, **(2013)**, pp. 529-541.
[18] Mobile Malware Report http://securelist.com/analysis/kaspersky-security-bulletin/58335/ mobile-malware-evolution-2013/, Last accessed 15 March 2015.
[19] Cisco Report 2014, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR. pdf, Last accessed 15 March 2015.
[20] Cyber Threats to Mobile Phones, https://www.us-cert.gov/sites/default/files/ publications/cyber_threats-to_mobile_phones.pdf, Last accessed 15 March 2015.
[21] T. Vidas, D. Votipka and N. Christin, "All Your Droid Are Belong to Us: A Survey of Current Android Attacks", **(2011)**, pp. 81-90.
[22] Android Users to Malware, http://researchcenter.paloaltonetworks.com/2015/03/android-installer-hijacking-vulnerability-could-expose-android-users-to-malware/, Last accessed 25 March 2015.
[23] Threats Report 2014, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf, Last accessed 25 March 2015.
[24] Internet Security Threat Report 2014, http://www.symantec.com/content/en/us/enterprise/
[25] other_resources/bistr_appendices_v19_221284438.en-us.pdf, Last accessed 25 March 2015.
[26] A. Portnoy, "Pwn2Own 2010", http://dvlabs.tippingpoint.com/blog/2010/02/15/ pwn2own-2010, **(2010)**.
[27] M. Keith, "Android 2.0-2.1 Reverse Shell Exploit", http://www.exploit-db.com/exploits/15423/.
[28] R. P. Weinmann, All Your Baseband Are Belong To Us, hack.lu, 2010,
[29] http://2010.hack.lu/archive/2010/Weinmann-All-Your-Baseband-Are-Belong-To-Us-slides.pdf.
[30] A. Greenberg, Google pulls app that revealed Android flaw, issues fix, 2010, http://news.cnet.com/8301-270803-20022545-245.html.
[31] [Mobile Cyber Threats, http://securelist.com/analysis/publications/66978/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/, , Last accessed 25 March 2015.
[32] M. Becher, "Security of smartphones at the dawn of their ubiquitousness", Ph.D. dissertation, University of Mannheim, **(2009)**.
[33] [31] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck and C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices". In Security and Privacy (SP), **(2011)**, pp. 96-111.
[34] K. Rosenfeld and K. Ramesh, "Attacks and Defenses for JTAG", IEEE Design & Test of Computers, vol.27, no. 1, **(2010)**, pp. 36-47.
[35] C. Boyd and P. Forster, Time and date issues in forensic computing—a case study. Digital Investigation, vol.1, no.1, **(2004)**, pp. 18-23.
[36] [34] F. C. Freiling, T. Holz and M. Mink, "Reconstructing People's Lives: A Case Study in Teaching Forensic Computing", In IMF, **(2008)**. pp. 125-142.
[37] C. Marforio, R. J. Masti, C. Soriente, K. Kostiainen and S. Capkun, "Personalized Security Indicators to Detect Application Phishing Attacks in Mobile Platforms", arXiv preprint arXiv:1502.06824, **(2015)**.
[38] H. Yao and D. Shin, "Towards preventing QR code based attacks on android phone using security warnings", In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, **(2013)**, pp. 341-346.
[39] J. Hubbard, K. Weimer and Y. A Chen, "Study of SSL Proxy attacks on Android and iOS mobile applications", In Consumer Communications and Networking Conference (CCNC), **(2014)**, pp. 86-91.
[40] [38]Mobile Threat Report 2014, https://www.f-secure.com/documents/996508/1030743/ Mobile_Threat_Report_Q1_2014.pdf, Last Access: 24 March 2015

Authors

Murat Yeşilyurt, He received the M.Sc. degree from Sakarya University, Turkey, in 2004 and he is currently working toward a Ph.D. degree at the same university in 2013. He is currently working as a lecturer at Turgut Ozal University in Turkey. His active research interests are information security, data hiding and image-video processing.

Yildiray Yalman, He received the M.Sc. and Ph.D. degree from Kocaeli University, Turkey, in 2007 and 2010, respectively. He is currently working as a lecturer at Turgut Ozal University in Turkey. His active research interests are data hiding, steganography, image processing and real-time multimedia communications.