ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20170627175835
Subject review

Vulnerability Analysis of Smart Phone and Tablet Operating Systems

Aysun COŞKUN, Ümit BOSTANCI

Abstract: New features are being added into mobile devices such as smart phones and tablets every day. Previously, people only used the phone for voice communication, but nowadays it allows almost any kind of internet operations even when travelling from one place to another. Smart phones and tablets are known to perform these operations through operating systems and application programs. Vulnerabilities may exist in the operating system or application software that allow these devices to be exploited by malicious users or hackers, by copying or deleting all of the data contained on them. For this reason, remediating the security vulnerabilities on operating systems is extremely important. In this study, a new database was created by querying security vulnerabilities of the most preferred operating systems on smart phones and tablets from National Vulnerability Database of the US and CVEDETAILS. With regard to vulnerabilities, CVSS scoring system, created by FIRST and used for scoring them, was examined in the light of re-scoring them. The analysis of security of the operating systems was done with quantitative methods. Eventually, it is aimed to conduct vulnerability analysis of smart phone and tablet operating systems.

Keywords: information security; operating systems; smart devices; tablet computers; vulnerability; zero-day vulnerability

1 INTRODUCTION

Mobile phones, when discovered, used to be relatively larger and only sent text messages together with making voice calls, and shrunk in size with improvements in microprocessor and chip technology, but became more functional in terms of added features. Today, almost all the operations, which can be done via a desktop computer, could also be done through smart phones and tablets, on the basis of basic functions. By means of the mobile devices, which are downsized enough to fit the size of a small pocket, simple operations such as bill payment and writing messages on social networks, as well as complex banking transactions and online shopping, can be made within minutes. When the main functions are taken into account, it can be said that both smart phones and tablets have an indispensable place in the life of human beings and their usage spreads day by day.

The number of broadband internet subscribers in Turkey, which was 6 million in 2008, increased by nearly eight times to 48.6 million as of September 2015. In addition, by September 2015, there were 73.2 million mobile, 64.2 million 3G and 37.4 million mobile internet subscribers [4]. According to the International Telecommunication Union (ITU) data it was estimated that the number of mobile broadband subscribers in the world, which was 268 million in 2007, would reach 3.6 billion by the end of 2016 [14, 15]. Considering the available data, it is also expected that the number of users and households connected to the internet will increase each day. Parallel to this increase in the number of users and devices, the security risks that may arise are expected to increase gradually.

The operating system is basic software located between the user and the hardware that allows the execution of various application software and is responsible for controlling all operations [5]. Smart phones and tablets have an operating system installed on them. Applications, which enable the ordinary users to easily perform operations, run on these operating systems. Not only in application software and operating systems, but also on hardware parts there may be various vulnerabilities allowing unauthorized use or access of smart phone and tablet resources. These vulnerabilities can be exploited by malicious users, the control of the device can be captured and all data on the device can be copied or deleted. But, deleted data can be retrieved by various forensics methods [13]. Data such as address books, text and voice messages, social networking messages, internet history and cookies, personal photos, videos, voice recordings and e-mails, internet banking passwords, can be obtained from smart phones and tablets. Actually, in recent days there have been many oral and written media reports about the private data, belonging to well-known people that are shared by third parties on the internet. While it is not known how these data were captured, it is possible to mention that vulnerabilities allow hackers to obtain them.

Nowadays, there are millions of smart phones and tablet computers with internet connection. In this regard, the hackers are able to access the data on them. Zero day vulnerabilities, which are not even known or noticed by the manufacturers, constitute the main point of attacks organized by hackers. In addition to zero day vulnerabilities, the systems will become suitable for exploitation if necessary precautions are not taken for publicly disclosed vulnerabilities.

2 DEFINITIONS AND BASIC CONCEPTS

In order to reduce risks associated with vulnerabilities, it is necessary to fix them on both operating systems and application software. Vulnerability is by Schultz [25] defined as a fault that allows attackers to overcome security measures. In addition, it is expressed as a failure or weakness in the operation, application or design of a system by Schneider [24]. Furthermore, it is also specified as the set of circumstances that allow an information system to be implicitly or explicitly infringed upon the confidentiality, integrity and accessibility of the information system [22]. International cybersecurity community, Common Vulnerabilities and Exposures (CVE), defines it as a flaw in the software that provides the ability to access the information, skills that can be used as "steppingstone" to access a system or network, or information accessibility and system configuration

problems [8]. The discovery of vulnerability can be identified by chance, as well as by professionals [7].

It has been revealed in a study that different vulnerabilities have different effects, that the potential risks of vulnerability can be quantitatively determined by Common Vulnerability Scoring System (*CVSS*), and that the risks posed by the security devices can be settled by the security personnel on that side [31]. In the researches about vulnerabilities it is observed that National Vulnerability Database (NVD), Exploit-DB, CVEDETAILS databases are used.

NVD, which was launched by National Institute of Standards and Technology (NIST) and MITRECorporation is growing day by day and still continues to function under MITRE's responsibility. It is known that NVD contains all CVEs currently disclosed and confirmed by software vendors [3] and all these CVEs are scored by *CVSS*. Thanks to the standards set by NIST, it is ensured common language is spoken and identifying the same problem in different ways by institutions or organizations is prevented. *CVSS* is a common framework designed to provide an open and standard method for scoring information system vulnerabilities [32]. With this system, the vulnerability scoring has been standardized and the risks can be prioritized [10].

There are three types of metrics in *CVSS*. The Base Metric Group, Temporal Metric Group and Environmental Metric Group are shown in Fig. 1. Each metric group is scored separately and takes a value ranging from 0 to 10. 0-3.9 indicates Low severity, 4.0-6.9 implies Medium severity, and 7.0-10.0 denotes High severity [20, 12]. *CVSS* base score calculation is shown in Eq. (1).

Generally, expressed as probability that an event, unpleasant or unwelcome, would happen in the context of information security, risk is confronted as something that can affect availability, confidentiality or integrity of business or personnel information [23]. In another definition, it is referred to as an exploited security vulnerability that has relative influence on the user's working environment [19]. The importance of risk is determined by considering the threat, vulnerability and asset value of the product. Hence risk can be calculated by multiplying asset, threat and vulnerability values [6].

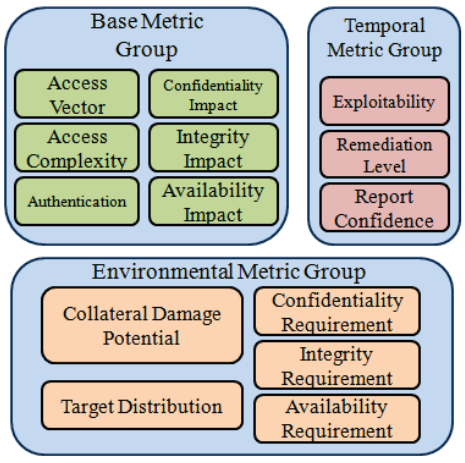

Figure 1 *CVSS* metric groups [19]

$$
\begin{aligned}
&Base\ Score = Round(((0.6*I)+(0.4*E)-1.5)*f(I))\\
&I = 10.41*(1-(1-CI)*(1-II)*(1-AI))\\
&E = 20*AV*AC*AU\\
&I = 0 \Rightarrow f(I) = 0;\ I\,!= 0 \Rightarrow f(I) = 1.176
\end{aligned}
\tag{1}
$$

Where: I - Impact, E - Exploitability, CI - Confidentiality Impact, II - Integrity Impact, AI - Availability Impact, AV - Access Vector, AC - Access Complexity, AU - Authentication.

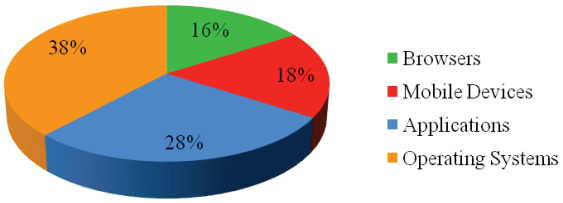

Figure 2 Distribution of the vulnerabilities discovered in 2015 [17]

In a study conducted in 2015, it was reported that an average of 25 vulnerabilities per day were added to NVD, 28% of these vulnerabilities belonged to application software, 16% to internet browsers, 38% to operating systems and 18% to mobile devices [17] (Fig. 2). In addition, considering the software vulnerability discovered in 2016, it was noteworthy that the most existed in Android with 523 vulnerabilities, the Debian Linux came second with 327, the Ubuntu Linux operating system was in the third place with 278, and iOS was the 15th with 161 [9].

Apart from published vulnerabilities, there are also some not shared with the public. The main issue causing damage to the information system assets of individuals and organizations is zero day security vulnerability not known by manufacturer, user, nor to the public until start of the attack [18]. Zero day vulnerabilities are used as the most effective weapon by hackers for cyber-attack because nobody is aware of them except for the discoverer. Since the updates released to fix the vulnerabilities are published after they are disclosed publicly, even the up-to-date systems can be captured by exploiting the zero-day vulnerabilities [11].

3 PREVIOUS STUDIES

Alhazmi and Malaiya, in a study conducted in 2005, analysed the vulnerability data of Windows NT and Windows 98 operating systems based on time. In consideration of data obtained, the usage preference of the operating system was divided into three phases and the vulnerability identification was associated with these phases. Phase 1, namely "learning phase", is the phase in which the information about the operating system was gathered and its features were understood. Phase 2 was named "linear phase". The operating system was used by more users and was gaining popularity by the users in that phase. "Saturation phase" was Phase 3. During this phase, the security patches of the operating system were issued less and the new operating system rather than the current one was preferred by the users. Within this scope, The Effort Based Model was developed under the assumption that the efforts made to identify vulnerability would increase when the operating systems became widespread

[2]. In this study, the basic 3-phase S-shaped model was presented in Fig. 3.

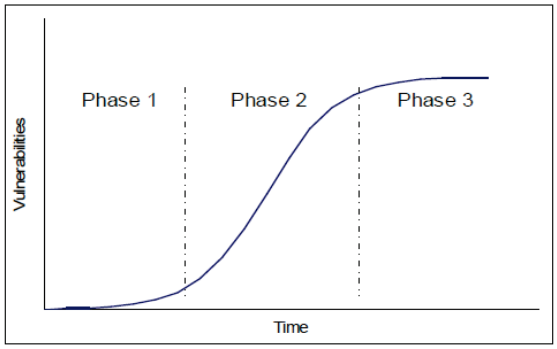

Figure 3 The basic 3-phase S-shaped model [2]

Schryen, with his study from 2009, introduced a theory named Mean Time Between Vulnerability Disclosure (MTBVD). According to this theory, the number of days per vulnerability was determined by dividing the number of days that lasted from the first issue of the operating system by the number of vulnerabilities detected up to that time. The vulnerability comparisons for open and closed source coded software were made accordingly. MTBVD also revealed the mean vulnerability detection time for the related software. Apart from this, it was emphasized in the study that the number of lines of the software was also an important factor for the vulnerability researchers. If the mean *CVSS* scores for the operating systems were compared, it would be seen Windows 2000 and Windows XP have the highest values with 7.20 score, then comes OSX as second with 6.80 score and the third ones were the Red Hat Enterprise Linux and Debian 3.1 version with 4.90 score. [26].

In the study done by Luo, Lo and Qu in 2014, it was stated that there were many vulnerability rating systems used by software developers, however *CVSS* was the only open system designed quantitatively. Besides, it was claimed that *CVSS* had some deficient aspects. To find a solution for this deficiency, they designed a new scoring system and called it Software Vulnerability Rating Approach. [SVRA] [16].

Al-Zadjali's study in 2015 aimed to analyse the vulnerabilities in respect to Android operating system. In this study, it was emphasized that Android was an attractive platform for hackers since it was open source. Moreover, the versions of this system were mentioned historically and its architecture was discussed. Apart from these, the vulnerabilities of this operating system were analysed based on years and vulnerability features. Besides, it was stated that the existing vulnerabilities could affect the users of this operating system, these vulnerabilities had to be closed by this system's developers, and hackers tried to leak to smart phones as well as computers [1].

4 METHODOLOGY

In this study, the most preferred operating systems are identified in smartphones and tablets, and the analysis is conducted in terms of security considering the vulnerabilities of these operating systems. Data was obtained from the globally accepted web sites, namely StatCounter and Netmarketshare. Statistical information was collected by taking into consideration Turkey and the World. The vulnerability data were acquired from the database developed by NIST and CVEDETAILS. The obtained data were transferred into a database. Then, vulnerabilities were re-scored according to well-accepted standards. They were analysed by considering also the usage rates. In this study, it is aimed to evaluate the tablets and smart phones' operating systems security vulnerabilities with quantitative methods.

For this, the steps followed were:

- Vulnerability and zero-day vulnerability terms were explained and the previous studies were examined.
- Common Vulnerability Scoring System [CVSS], issued by FIRST and used as a common standard in the world, was studied.
- Considering the data obtained from June 2015 to June 2016, the most commonly used operating systems for smart phones and tablets in the world and Turkey were determined via searching in the web sites named StatCounter and Netmarketshare.
- The vulnerability data of these operating systems found in NVD and CVEDETAILS of the USA were transferred into a database set in MS Access, then the exploitability of vulnerabilities and the risk levels were calculated in consideration of obtained data and the equalities determined in *CVSS*.
- An analysis was carried out by taking into account the operating systems' usage rates.

5 FINDINGS

In this study, the most preferred operating systems on smart phones and tablets as well as the *CVSS* values of their security vulnerabilities were analysed.

5.1 The Most Preferred Operating Systems

The most commonly used smart phone and tablet operating systems in Turkey and in the World were identified in terms of data received from StatCounter and Netmarketshare web sites.

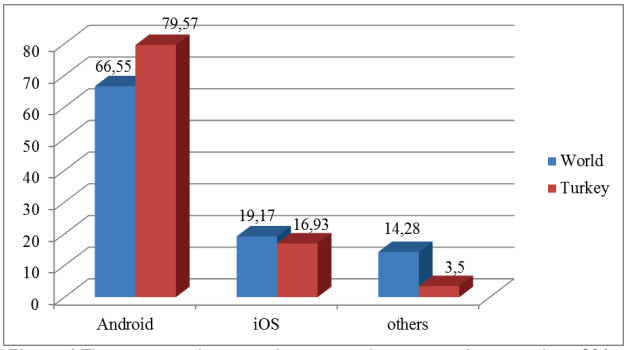

Figure 4 The most popular smartphone operating systems between June 2015 and June 2016 [27, 28]

According to Fig. 4 the most popular smart phone operating systems are Android with 79.57%, iOS with 16.93% and the others in Turkey, in the world with 3.5%; Android leads the market with 66.55%, iOS ranks second with 19.17%, and the others 14.28%.

As for Tablets in Fig. 5; operating systems are Android with 63.76%, iOS with 35.99% and the others in Turkey with 0.25%. In the world Android leads the market with 65.64%, iOS ranks second with 32.10%, and others 2.26%.

Similarly, according to Netmarketshare 58.38% of Android, 33.99% of iOS and 7.63% of others are used in the smart phones and tablets.

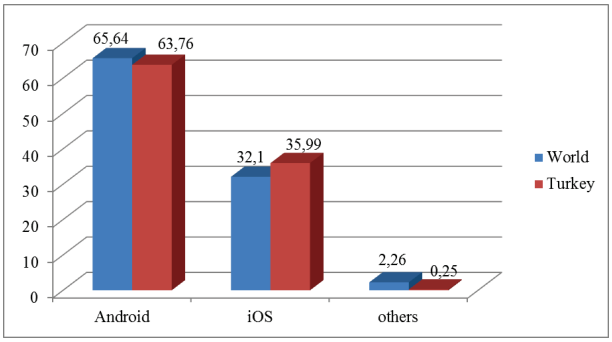

Figure 5 The most popular tablet operating systems between June 2015 and June 2016 [29], [30]

5.2 Vulnerability Analysis of Operating Systems

In this part of the article, vulnerabilities in the operating systems were analysed by taking the data from pioneering NVD database, the source of many web pages and organization publishing vulnerability data. The "cvedetails.com" web page referring to the NVD as the source of the data was used in this study.

First of all, the collected data was transferred into a new database. Then, 1224 vulnerability data published from the release date of operating systems until 30 June 2016 were accumulated and analysed. After that, data were collected, recalculated according to the *CVSS*' Base Scores, and results were compared whether or not there were any discrepancy between the collected data and the scores disclosed on the web page. Finally, the collected data were filtered according to various criteria and then analysed.

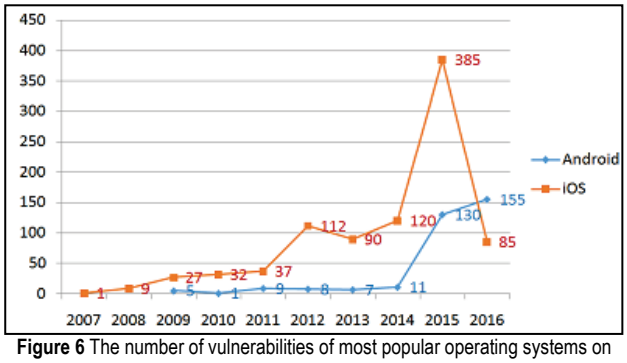

Figure 6 The number of vulnerabilities of most popular operating systems on smart phones and tablets based on years

In the light of the data, Android has 326 and iOS has 898 vulnerabilities. Hence, the usage rates are taken into consideration, iOS has 2.7 times higher value than Android, even though Android is much more preferred than iOS. In addition, there has been serious increase in terms of the vulnerabilities of both iOS and Android since 2015.

The amount of vulnerabilities disclosed on a yearly basis for most preferred operating systems in smart phones and tablets is given in Fig. 6 and Tab. 1. It is noteworthy that iOS experienced a considerable increase in 2012, and a substantial increase in 2014 and 2015, despite a slight decrease in 2013. However, despite the fact that Android experienced a significant increase in 2015 and 2016 in terms of amount of vulnerability, 155 vulnerabilities were disclosed in the first half of 2016. It is known that this number reached 523 at the end of the year. By contrast, the number of vulnerabilities of iOS, which was 85 in the first half of 2016, reached 161 by the end of the year. While the number of vulnerabilities of iOS was apt to decline in the first half of 2016, the amount of Android was prone to rise during the same period.

Table 1 Vulnerabilities of the most used operating systems by years

Amount of vulnerabilities			
Years	Android	iOS	Total
2007	-	1	1
2008	-	9	9
2009	5	27	32
2010	1	32	33
2011	9	37	46
2012	8	112	120
2013	7	90	97
2014	11	120	131
2015	130	385	515
1st half of 2016	155	85	240
Total	326 (%26.63)	898 (%73.37)	1224

When the average *CVSS* of the vulnerabilities of the most used smart phone and tablet operating systems are taken into account, it is observed that Android has a higher value with 7.882 than iOS, with value of 6.230. In addition, when average exploitability values are taken into consideration, it is seen as in Tab. 2 that Android is higher - 8.378 than iOS, with value of 7.848.

Table 2 Mean values of operating systems by *CVSS* and exploitability scores

Operating systems	Average *CVSS* base scores	Average *CVSS* exploitability scores
Android	7.882	8.378
iOS	6.230	7.848

In Tab. 3, when the average duration between vulnerabilities of the most used operating systems in smart phones and tablets is taken into consideration, iOS disclosed vulnerability during 3.368 days, compared to 8.558 for Android. It is estimated that the risk of these operating systems decreases, the risk value and invention of vulnerability are directly related to the usage rates, as the average duration between vulnerabilities increases.

Table 3 Average duration between vulnerabilities.

Operating systems	OS publishdates	The last vulnerability publish dates	Average durati on between vulnerabilities (days)
Android	22.10.2008	12.06.2016	8.558
iOS	08.03.2008	19.06.2016	3.368

The usage rates in Tab. 4 and Tab. 5 are the rates of the most preferred operating systems on smart phones and tablets in Turkey. Considering the risk values calculated here Android ranks first with 0.732, iOS has a value of 0.313.

As for Tab. 5, while iOS ranks first with 0.655 for tablets, Android comes second with 0.587. It is evaluated

that, as the average duration between vulnerabilities increases, the risk of that operating system decreases and the risk value and invention of vulnerability are directly related to the usage rates.

Table 4 Risk calculated by average CVSS and usage rate for smartphones

Operating systems	Average *CVSS* base score - *V*	Usage rates - *UR*
Android	7.882	0.7957
iOS	6.23	0.1693
Operating systems	*ADBV* (Days)	*Risk = V*UR/ADBV*
Android	8.558	0.732
iOS	3.368	0.313

Table 5 Risk calculated by average *CVSS* and usage rate for tablets

Operating systems	Average *CVSS* base score - *V*	Usage rates - *UR*
Android	7.882	0.6376
iOS	6.23	0.3599
Operating systems	*ADBV* (Days)	*Risk = V*UR/ADBV*
Android	8.558	0.587
iOS	3.368	0.665

Considering the data in Tab. 6, the most noticeable point is that the amount of vulnerabilities of iOS is higher than Android, but 69.01% of Android has a high level of *CVSS*. On the other hand, it is observed that 60.02% of iOS has a medium level, and 28.17% of high level of *CVSS*.

Table 6 Operating systems' *CVSS* base score by severity.

Operating systems	Low (0-3.9)	Medium (4.0-6.9)	High (7.0-10)	Total
Android	8 (2.45%)	93 (28.52%)	225 (69.01%)	328
iOS	106 (11.80%)	539 (60.02%)	253 (28.17%)	898
Total	114	632	478	1224

When Tab. 7 is examined it will be seen that Android has more vulnerabilities in terms of *CVSS* in the critical level. It is clear that the majority of these vulnerabilities in Android have been published since 2015. The same situation is also valid for iOS, and disclosure of critical levels has increased after 2015, but has declined in the first half of 2016.

Table 7 Distribution of critical vulnerabilities (*CVSS* = 10) of operating systems by years

Amount of vulnerabilities of OS			
Years	Android	iOS	Total
2008	-	1	1
2009	-	1	1
2010	-	2	2
2011	1	-	1
2012	-	1	1
2014	-	4	4
2015	61	9	70
1st half of 2016	24	3	27
Total	86	21	107

It has been determined that only 2 of 1224 vulnerabilities of operating systems used on smart phones and tablets are the same in Android and iOS, and the remaining 1220 are found in only one in each operating system. Amounts of them are 324 for Android, and 896 for iOS.

6 CONCLUSIONS

The technological devices such as smart phones and tablets added to the cyberspace not only help us to make our lives easier with their increasing efficacy, but also cause some security problems we do not want. Although the security updates are published by the manufacturer as quickly as possible to remediate vulnerabilities, it is known that security updates cannot be done correctly by some users. An operating system that has vulnerability not patched increases the appetite of hackers, and the individuals using this operating system can also be victimized. In recent years, the data from smart phones and tablets of the famous people were captured and served to the media. A number of personal protective precautions can be taken by providing passwords, scrolling patterns, and fingerprint access to mobile devices. However, these measures do not prevent hackers from remotely accessing mobile devices. In order to improve the security measures, it is necessary to fix the vulnerabilities that allow remote access and control of hackers. Not to remediate the vulnerability brings about violation of privacy, integrity and accessibility causing both financial and emotional damage. Even though it is not possible to completely eradicate these damages, it is considered that the most possible harms can be reduced by appropriate security measures taken in advance. It should not be forgotten that every vulnerability, not properly patched, will augment the risk of an attack.

The security updates released by software producers to fix the vulnerability must be done using methods advised by the manufacturer. It is being recommended that restrictions (jailbreak/root) on mobile devices should never be removed and security updates should not be downloaded from third party sources. It is extremely important to provide security to the operating systems which make resource allocations to the other applications running on the device. However, ensuring solely the security of the operating system does not mean that the device is completely secure. Because of security vulnerability in application software the devices can be exploited. For this reason, the sensibility shown to fix the vulnerabilities of operating systems must also be done to the other applications.

CVSS provides a framework that allows for the appraisal of software vulnerability using quantitative methods. Through a common evaluation system such as *CVSS*, corporates and institutions can conduct objective risk assessments of their assets.

In this study, the most used smart phone and tablet operating systems are identified and analysed in terms of vulnerabilities. *CVSS* values of these operating systems are taken into consideration. Furthermore, the usage rates of the operating systems and the average duration between vulnerabilities are taken into account. Although iOS operating system has more vulnerability in terms of quantity, as a result of the analysis, it is conceived that Android has a higher *CVSS* score in terms of quality, a significant increase in the number of faults detected for Android in 2016, and decline in the number of vulnerabilities for iOS. However, as long as the operating systems are used, vulnerabilities will be discovered. It is evaluated that vulnerability rates are directly related to

usage rates; undesirable operating systems are not the target platform for vulnerability researchers. As the release period of vulnerability becomes longer, the risks of the operating systems will be decreased. The analyses explained in this study will be beneficial for people and institutions, using mobile devices, in terms of making security evaluations of their assets.

7 REFERENCES

[1] Al-Zadjali, B. M. (2011). A Critical Evaluation of Vulnerabilities in Android OS: (Forensic Approach). *International Journal of Computer Applications, 130*(5), 38-42. https://doi.org/10.5120/ijca2015907005

[2] Alhazmi, O. H. & Malaiya, Y. K. (2005). Quantitative Vulnerability Assessment of Systems Software. *Annual Reliability and Maintainability Symposium* / Virginia, USA. https://doi.org/10.1109/RAMS.2005.1408432

[3] Allodi, L. & Massacci, F. (2012). A Preliminary Analysis of Vulnerability Scores for Attacks in Wild the EKITS and SYM Datasets. *Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security Conference* / North Carolina, USA. https://doi.org/10.1145/2382416.2382427

[4] (2016). Information and Communications Technologies Authority. *Turkey Electronic Communications Sector Quarterly Market Data Report*. Ankara, Turkey, vol. VI, 40-41.

[5] Brookshear, G. J. (2012). *Computer Science an Overview*. 11th Ed. New York: Pearson Addison-Wesley, 124.

[6] Caballero, A. (2009). *Information Security Essentials for IT Managers: Protecting Mission-Critical Systems*. Computer and Information Security Handbook / John R. Vacca. 1st Ed. Burlington, USA, Morgan Kaufmann Publishers, 231-232. https://doi.org/10.1016/B978-0-12-374354-1.00014-5

[7] Coşkun, A. & Bostancı, Ü. (2016). Evaluation of The Most Preferred Operating Systems on Computers in Terms of Vulnerabilities. *International Journal of Human Sciences, 13*(3), 4545-4564. https://doi.org/10.14687/jhs.v13i3.4128

[8] (2016). CVE (Common Vulnerabilities and Exposures). Terminology. Vulnerability. http://cve.mitre.org/about/terminology.html (26.06.2017).

[9] (2016). CVEDETAILS. Top 50 Products by Total Number of Distinct Vulnerabilities in 2016. https://www.cvedetails.com/top-50-products.php?year=2016. (26.06.2017).

[10] (2015). FIRST. Common Vulnerability Scoring System v3.0: Specification Document. USA, 1-21.

[11] Garcia, M., Bessani, A., Gashi, I., Neves, N., & Obelheiro, R. (2014). Analysis of Operating System Diversity for Intrusion Tolerance. *Software: Practice and Experience, 44*(6), 735-770. https://doi.org/10.1002/spe.2180

[12] Ghani, H., Luna, J., & Suri, N. (2013). Quantitative Assessment of Software Vulnerabilities Based on Economic-Driven Security Metrics. International Conference on Risks and Security of Internet and Systems / La Rochelle, France, 23-25. https://doi.org/10.1109/CRiSIS.2013.6766361

[13] Güllüce, Y. Z. & Benzer, R. (2015). Hard Disk Failure and Data Recovery Methods in Computer Forensic. *International Journal of Human Sciences, 12*(1), 206-225. https://doi.org/10.14687/ijhs.v12i1.3115

[14] (2016). International Telecommunication Union (ITU). ICT Fact and Figures 2016. Geneva, Switzerland, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf. (26.06.2017).

[15] (2016). International Telecommunication Union (ITU). Key ICT indicators for developed and developing countries and the world. Geneva, Switzerland, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/ITU_Key_2005-2016_ICT_data.xls. (26.06.2017).

[16] Luo, J., Lo, K., & Qu, H. (2014). A Software Vulnerability Rating Approach Based on the Vulnerability Database. *Journal of Applied Mathematics*, (932397). https://doi.org/10.1155/2014/932397

[17] Manes, C. 2015's MVPs – The most vulnerable player. http://www.gfi.com/blog/2015s-mvps-the-most-vulnerable-players/. (26.06.2017).

[18] McQueen, M. A., McQueen, T. A., Boyer, W. F., & Chaffin, M. R. (2009). Empirical Estimates and Observations of 0 Day Vulnerabilities. *Hawaii International Conference on System Sciences* / Hawaii. https://doi.org/10.1109/HICSS.2009.186

[19] Mell, P., Scarfone, K., & Romanosky, S. (2007). A Complete Guide to the Common Vulnerability Scoring System Version 2.0. FIRST, USA, 1-23.

[20] (2016). National Vulnerablity Database (NVD). NVD Common Vulnerability Scoring System Support v2. https://nvd.nist.gov/cvss.cfm. (26.06.2017).

[21] (2017). Netmarketshare. Market Share Statistics for Internet Technologies. http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1&qpsp=197&qpnp=13&qptimeframe=M. (26.06.2017).

[22] (2004). NIAC. Vulnerability Disclosure Framework Final Report and Recommendations by the Council. NIAC, USA, 7-13.

[23] Rao, U. H. & Nayak, U. (2014). *The infosec handbook an introduction to information security*. Apress Media, New York, 79. https://doi.org/10.1007/978-1-4302-6383-8

[24] Schneider, F. B. (1999). *Trust in Cyberspace*. National Academy Press, Washington D. C., 13.

[25] Schultz, E. E., Brown, D. S., & Longstaff, T. A. (1990). *Guidelines for Incident Handling*. United States, 55.

[26] Schryen, G. (2009). Security of open source and closed source software: An empirical comparison of published vulnerabilities. *Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS)* / San Francisco, California.

[27] (2016). StatCounter. Top 8 Mobile Operating Ssystems in Turkey from June 2015 to June 2016. http://gs.statcounter.com/#mobile_os-TR-monthly-201506-201606-bar. (26.06.2017).

[28] (2016). StatCounter. Top 8 Mobile Operating Ssystems from June 2015 to June 2016. http://gs.statcounter.com/#mobile_os-ww-monthly-201506-201606-bar. (26.06.2017).

[29] (2016). StatCounter. Top 7 Tablet OSs in Turkey from June 2015 to June 2016. http://gs.statcounter.com/#tablet-os-TR-monthly-201506-201606-bar. (26.06.2017).

[30] (2016). StatCounter. Global Stats. Top 7 Tablet OSs from June 2015 to June 2016. http://gs.statcounter.com/#tablet-os-ww-monthly-201506-201606-bar. (26.06.2017).

[31] Wang, R., Gao, L., Sun, Q., & Sun, D. (2011). An Improved CVSS-Based Vulnerability Scoring Mechanism. *3rd International Conference on Multimedia Information Networking and Security* / Shanghai, China. https://doi.org/10.1109/MINES.2011.27

[32] Zhang, S., Caragea, D., & Ou, X. (2011). An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities. *22nd International Conference on Database and Expert Systems Applications (DEXA)* / Heidelberg, Germany. https://doi.org/10.1007/978-3-642-23088-2_15

Contact information:

Aysun COŞKUN, Assoc. Prof.
Gazi University,
Faculty of Technology,
Department of Computer Engineering,
Teknikokullar - 06500- Ankara, Turkey
aysunc@gazi.edu.tr

Ümit BOSTANCI
Gazi University,
Informatics Institute,
Department of Computer Forensics,
Tunus Cad. No: 35 Kavaklıdere, Çankaya/Ankara, Turkey
umit.bostanci@hotmail.com