Mobile Application Security Platforms Survey

Sardasht M. Mahmood
Statistics and Computer Dept.
College of Commerce
University of Sulaimani
Sulaimani, Iraq

Bakhtiar M. Amen
Dept. of Informatics, School of Computing andEngineering
University of Huddersfield
United Kingdom

Rebwar M. Nabi
Department of IT
Computer Science Institute
Sulaimani Polytechnic University,
Sulaimani, Iraq

ABSTRACT
Nowadays Smartphone and other mobile devices have become incredibly important in every aspect of our life. Because they have practically offered same capabilities as desktop workstations as well as come to be powerful in terms of CPU (Central processing Unit), Storage and installing numerous applications. Therefore, Security is considered as an important factor in wireless communication technologies, particularly in a wireless ad-hoc network and mobile operating systems. Moreover, based on increasing the range of mobile application within variety of platforms, security is regarded as on the most valuable and considerable debate in terms of issues, trustees, reliabilities and accuracy. This paper aims to introduce a consolidated report of thriving security on mobile application platforms and providing knowledge of vital threats to the users and enterprises. Furthermore, in this paper, various techniques as well as methods for security measurements, analysis and prioritization within the peak of mobile platforms will be presented. Additionally, increases understanding and awareness of security on mobile application platforms to avoid detection, forensics and countermeasures used by the operating systems. Finally, this study also discusses security extensions for popular mobile platforms and analysis for a survey within a recent research in the area of mobile platform security.

General Terms
Mobile Platform Security, Information Security & Trust, Mobile OS Security.

Keywords
Threats, cyber strategy, mobile platforms, security, security awareness, sensitive data and vulnerability.

1. INTRODUCTION
Currently Smartphone and mobile devices have become incredibly important among people around the world. Because they have offered same capabilities as well as facilities that desktop works stations have provided. However, security aspect still is a big Challenge [22]. Nowadays, the numbers of attackers and malicious programs have increased rapidly. According to threats predictions report [24] 2015 will the turning point for threats to mobile devices in which the total number of mobile malware samples exceeded 5 million in Q3 2014. Therefore, security requirements and issues within various mobile platforms become a targeted area of many studies and researches. Thus, one of the most essential decisions within the use of Smartphone is the selection of suitable mobile platforms. Generally, confidentiality, integrity and availability are three fundamental categories of the security goals and objectives of information in an organization [3] [17]. More to say, security can be measured through: 'confidentiality, integrity, authentication and authorization' [15]. Moreover, risk analysis is also considered as one of the main crucial factors within security of mobile platforms. In addition to these, when security issues and gaps are subsisted, it is crucial to identify the challenges against existed security issues [30]. Due to incredible increasing of memory, data transmission and processing the security incident turned into be more powerful on mobile platforms and phone devices [2].

This paper will focus on security in mobile application platforms and techniques for analysis and prioritization of security requirement In terms of theory rather than technical descriptions. Furthermore, the analysis and evaluation of the existing techniques and studies will be presented. This study introduces both 'generic model security architectures' and 'threat model' of mobile platforms within two major known platforms of iOS and Android. The last but not the least, the security issues and privacy in mobile platforms will be also discussed.

It is worth mention that in this paper, security in mobile platforms has been analyzed in different perspectives in which it identify how both iOS and Android platforms has implemented security models against threats.

This paper organized as it follows; in section II presents the importance of this study, section III presents Background of mobile platforms, section IV introduces mobile application security platforms, namely the (i) the Rational behind securing mobile application platforms, and (ii) security threats measurements. Finding and evaluation are provided in section V and VI respectively. Finally, the conclusion of the paper will be presented.

2. THE IMPORTANCE OF THIS STUDY
Currently Smartphone and mobile device have become the most targetable sources for hackers and malicious program. According the threat prediction report from McAfee Labs in Q3 2014 the total number of mobile malware samples exceeded 5 million. Moreover, about 110 million Americans— equivalent to about 50% of US adults—have had their personal data exposed in some form in the past year. Therefore, it can be identified it is essential to have the state-of-the-Art about how mobile platforms provide security mechanism. Consequently, people will have right materials to choose the right platform to use daily. Finally, this survey will help platform providers to improve their security mechanism based on the finding of this study.

3. BACKGROUND
Every year the size of mobile market increased significantly, while mobile phone user's subscriptions estimated 7,084,987 billion by 2015 based on the ITU report in [20]. Each mobile platform introduced and implemented their models or approaches to enforcing application security. Attack goals, attack vectors and mobile malware are three classified sections of threat model within mobile platforms [10] as shown in figure 1.

Generally, security is defined as "the capability of software to prevent deliberate or inadvertent unauthorized access to code or data" [5] [6]. In practice, 'security aspects are categorized by: Authenticity, Confidentiality, Integrity, Accountability, and Availability' [5] [6]. Furthermore, security requirement is one of the emergent areas for the researchers to focus on within mobile platforms due to emerging enormous numbers of mobile applications within different mobile platforms. Likewise, developers are most likely concentrates on security constraints during some of the processes (phases) within the various mobile application models and methodologies.

Although mobile is a personal device that would be trustful for whom that will use the application within the mobile for doing different actions. Transferring the patient's sensitive information to the external servers is one of the essential concerns from therapists or doctors [23] [27], [33]. Despite that reason, the increase in using mobile applications for different aspects needs an essential level of security due to the existence of availability services and sensitive information inside mobile applications [9] [28]. In addition, having many threats, unauthorized access to the information through mobile and avoid internal access to stored information authentication process for mobile application is required.

Confidentiality, availability and integrity are considered as three main crucial requirements that each system should have to secure the data and provide the appropriate security solutions. Confidentiality insures that the information will not reach to wrong destination, while it must also guarantees that right people obtain the right data. Availability refers "prevention and recovery from hardware and software errors and from malicious data access denials making the database system unavailable" [27]. Integrity refers preventing systems in data modification from unauthorized and improper behavior [27].

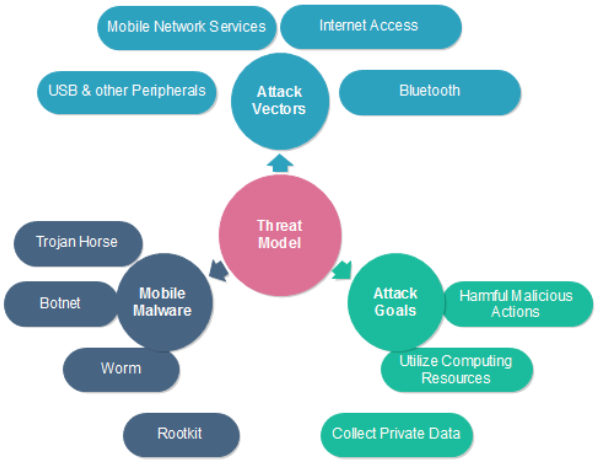

Fig 1 : Mobile Platform Model Threats (MPMT) [10]

Furthermore, growing and expansion of mobile applications and platforms, security concerns are raising in different aspects of our life [7]. Information security, system security, network security, and physical security are the four fundamentals of security in mobile computing. Meanwhile, the accessibility attempted to be the essential features of mobile clouds computing to be able to access to data from anywhere and anytime. Currently, mobile platform enterprises are requiring restricted security mechanisms from IT companies and technology infrastructures with implementing new levels of security in order to protect user's data. In the meantime, existing technologies for the security can be embedded within mobile platforms architecture such as 'firewalls, authentication servers, biometrics, cryptography, and Virtual Private Network' [8].

4. MOBILE APPLICATION SECURITY PLATFORMS

Mobile application development in various platforms is based on functional and non-functional requirements [17]. Currently various types of platforms are exist to deploy mobile applications with different private policies. Therefore, this research focuses on the most priceless and popular mobile application platforms in the worldwide. Furthermore, it discusses that how the security within each platform is different from each others for instance, Motion BlackBerry OS, Apple iOS, Google Android, Microsoft Windows Phone. There are some of the imperative security issues to be evaluated and studied such as 'battery capacity limitation', and 'encryption algorithms power consumption', were having major impacts on mobile devices [35].

In addition to these, controlling third-party application is difficult task within each mobile apps store, which they have huge impacts on increasing the security issues within mobile platforms. Dimensional Research institution in [11] stated that 'Android trusted less; Windows Mobile and BlackBerry trusted more for security'. Meanwhile, based on the same survey or report accordingly, most of participants believed that the security risks were the major cause of the mobile security platforms. The number of IT professionals saying Android was the riskiest increased and was by far the most frequent platform indicated (64%). Moreover, Apple/iOS followed Android by (16%) and Windows Mobile (16%) and Blackberry (4%). Perception of Android security problems continued to grow theatrically as the platform perceived to have the greatest security risk (up from 49% in 2013 and 30% in 2012) [11].

4.1 The Rational behind Securing Mobile Application Platforms

The major risks which have made mobile platforms been attractive targets for attacks and threat were from unknown publisher (developer). Meanwhile, web based applications were supported by some of the most popular mobile platforms such as Windows Phone 8, iOS, and Black Berry 10 [1], Mobile Web browser applications are facing the same security threats on Web View Technology like computers in terms of having all the vulnerabilities [29]. 'Application layer', Middleware layer' and 'Kernel layer' are vital extension layers that have been recommended against privacy and security issues within different mobile platforms [1]. In addition, differences within mobile platforms for instance the security architectures are based on a similar model; Permission-based access control, code signing, and application isolation are the three fundamental built security techniques within various mobile platforms [1].

It is worth mentioning that in the past mobile platform companies were mostly focused on development features rather than other essential concepts such as security. For that reason, platform weakness, storage and binary were misused [25], while Data storage includes key stores, application file system, application database, caches and configuration files. Binary consist of 'embedded credentials and 'key generation routines.

Furthermore, numerous of research papers have been published with related of mobile security and the effective of malicious application on different mobile platforms. At the

same time, banking applications were one of the priority targeted area for attackers to gain financial benefits and personal data (personal information, cardholder data). Nonetheless, the attempt is based on attack to breach restrictive application licensing and functionality and restrictive platforms [25]. Meanwhile, getting famous and embarrassing people are the other purposes of the hacker's interests. Finally, other attack destinations include platform, malware installation, mobile botnets and Application architecture decisions based on platform [25].

4.2 Security Threats Measurement

There are some principal security measurements which needed to be concerned, for technical solutions for mobile agents such as Encryption, Digital signatures and certificates, Central management of access permissions, Sandbox and Secure communication channels [6].

In fact, core processes and business models can be transferred through the revolution of mobile devices (Smartphone). It is evident that security is one of the essential sections within life cycle of application management. Recent study reported that one of the most concerns within mobile technology and mobile system is security. According to Finneran in [13] states that onboard encryption is not supported by various mobile operating systems and its versions. In addition, SSL-based access and VPN are some of the possible solutions to avoid obtaining sensitive data. Besides, in [18] based on the survey that conducted by information week for 343 business technology professionals, the top concerns over growing number of devices and platforms clarified as:

- Security risks
- Numbers of devices and platforms
- Lack of maintenances

5. FINDING

The security model within mobile platforms or mobile-OS can be compared based on traditional access control approaches, application provenance, encryption, isolation (sandboxing), and access control [4]. Moreover, mobile malware, web- and network-based are known as the important types of threats within mobile security, Bhattacharya, et. al in [4] categories the fundamentals of mobile security in mobile-device security and privacy, mobile-app security, mobile network and communication security.

Furthermore, security mechanisms were implemented against malicious intentions within iOS applications through professionals and code reviewers. Meanwhile, it makes safe side to download and install an application on the App Store. Android platform have its own procedure action called application isolation in which, an application is prevented to hold up with other applications [10]. It is widely accepted that there are lots of worms are recently existed and affected mobile platforms for instance Ikee.B is one of the examples of stealing sensitive data from jailbroken iPhones [10]. Permission based security model has also been implemented within Android platform to deal with security issues as depicted in figure 2.

Other studies like Asokan et. al in [1] introduced Privilege-escalation attacks, detection of malicious applications and application hardening. Based on the literature study within mobile platforms security attacks and threats were classified into three main sections such as Privilege Escalation, Malicious Applications and Risky In-App Ad Libraries as depicted in table 1.

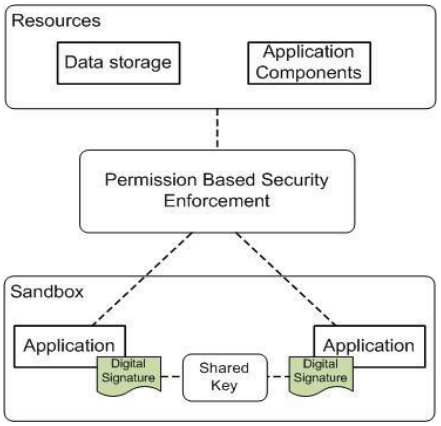

Fig 2: Android Security Model [10]

Table 1. Attacks and threats [1]

Attacks & Threats	Description
Privilege Escalation	- Beyond its authorizations, data can be accessed and operated through an application based on this attack - This attack is totally different within various mobile platforms.
Malicious Applications	- Mobile platforms is a targetable area to malware attacks because various mobile platforms have powerful ability to store a large amount of data (sensitive) - Based on the researches and articles there are some of the malware threats have been addressed such as by static and dynamic analysis of application binaries, enhanced application installers, novel run-time privacy frameworks and app store analysis tools.
Risky In-App Ad Libraries	- Evaluate potential privacy and security risks - An advertisement library is a part of the apps, that the app developers integrate it.

Moreover, when the mobile device stolen or lost the security risks alert. Buffer overflow is still one of the vulnerabilities within an Apple's application besides the advantages of having vetting process (it is a process to review the apple's application). It can be said that with entire dedicated site as a guideline for the developers and Objective-C in iPhone programming language [1] [12]. Likewise, vetting process is not a concrete solution against malicious actions due to the existence of different approaches to hide the malicious codes in applications [1] [34]. Hence, vetting process has not been provided by the Android platforms for the developers. Similarly, Google initiate the guidelines for both users and developers for the security reasons [12].

Unlike mobile web application, security and testing in native mobile applications are more motivating [13], for that reason, mobile platform manufacturers are supposed to build secure applications/device and a 'secure process for issuing platform software' [15]. It is widely accepted that within mobile platforms various critical architectural security components

has been implemented such as 'software and hardware security architecture'. Nonetheless, performance, security and scalability are three main properties of mobile platform, which manufactures should concern about [6]. Bhattacharya et. al in [4] emphasized that security in mobile operating system consists of "threats to", "attacks on", and defenses, those aspects should be covered includes: secure coding, cryptography, physical security, secure communication, and policy management.

It is widely known that mobile devices in terms of hardware and operating system (OS) are main targeted area for attacking[2] [10]. "Companies and individuals are skeptical of allowing an uncontrollable piece of code to be loaded onto their machines and execute, which is basically what a virus does" [6] [16]. According to a statistical study the available apps to download in popular mobile stores is remarkably surprising which ended by 1.6 millions of apps in Google play store by July 2015. Additionally, the apple store has 1.5 million of app available according to the same study, while the windows phone and BlackBerry world have 400,000 and 130,000 respectively [32]. The rationale behind mobile threats and malicious exploits is based on having large numbers of application and expectation for movements and having a different OS for mobile phones as predicted in figure 3.

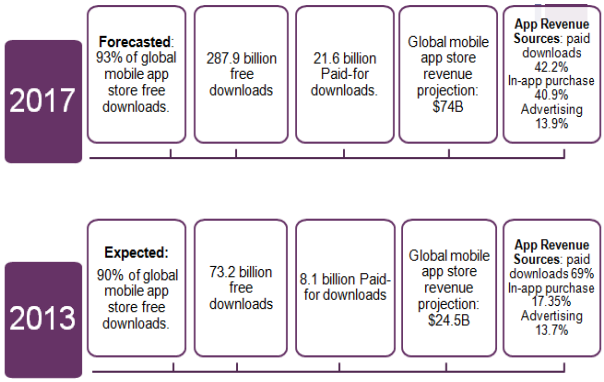

Fig 3: Mobile App Store Trend adopted [26]

Moreover, potential threats are more likely to be diverse from the different stakeholder's perspectives. In addition, 'secure and reliable communication' 'mobile network operator', and 'content providers' are stakeholder's primarily classes [15], each mobile platform should have or implement a mechanism to provide essential security. The vital security functions has been clarified such as "secure boot and software integrity, secure control of debug and trace capabilities, digital rights management, hardware cryptographic accelerators, hardware-based random number generator, cryptographic algorithm service, public key infrastructure support and secure communication protocols" [15]. Mobile platform may behave securely when the integrity of core platform software and critical data guaranteed as well as the mobile device platform must contain security functions that guarantee secure execution and code integrity.

Today, mobile application is developing continuously in mobile platforms. Malicious exploit attacks on hardware and OS like personal computer (PC) as well as mobile platforms threats including Trojan horse, worm, virus and malicious application have been increasing dramatically [10]. For that reason, Smartphone user's privacy and security is compromised. In fact, above mentioned types of threat have vital impact on controlling the device's voice recording, cameras, short message service (SMS), Global Positioning System (GPS), services and mobile payments.

Through, emerging numerous features for Smartphones within different platforms, new types of security issues and security concerns have faced mobile users. Each mobile platform should have a critical solution for the security issues in order to achieve user's protection and security for their mobile devices. Unlike Android application platform, iOS application platforms had a revision process for each new application to be released in application store [10].

There are some of the diversity between the PC windows and mobile platforms such as integration within IT architecture and third party security products. In Both aspects PC is regarded as more secure compare to mobile platforms. Hence, many mobile platforms infrastructures have applied several important policies as well as procedures such as authentication and authorization to provide secure platforms against threats. Some researchers discussed that allowing right user to access the devise and losing sensitive information or data stored on mobile device are the key concern that necessary to be considered against threats on mobile enterprise [28]. Table 2 provides an overview of global Smartphone plat forms sales to end-users in August 2015.

Table 2. Market Share Analysis [19]

Operating System	2015Q2	2014Q2	2013Q2	2012Q2
Android	82.8%	84.8%	79.8%	69.3%
iOS	13.9%	11.6%	12.9%	16.6%
Microsoft	2.6%	2.5%	3.4%	3.1%
Blackberry	0.3%	0.5%	2.8%	4.9%
Other OS	0.4%	0.7%	1.2%	6.1%
Total	**100.0**	**100.0**	**100.0**	**100.0**

As it can be seen from above table the Android OS is controlling the market share for years 2012, 2013, 2014, 2015 consecutively. However, iOS is taking the second place since 2012Q2, while the other OSs is coming after them. It is worth mentioning that OSs like Windows phone and Blackberry losing the market share considerably from 2012 to 2015.

6. EVALUATION

Unlike iOS and other platforms, Blackberry enterprise server administrator has ability to implement a uniform security policy which is impossible for Uniform security policy PIN protection and data encryption overridden by the users [28]. In addition, it does not allow sensitive data to be in vulnerable state. While, in the iPhone and other mobile devices the data could be vulnerable. Permissions are one of the critical differences within iOS and Android platforms [10]. In the former, an application can be installed in iOS platform through App Store which might has permissions to use and access mobile device's Wi-Fi, Camera and others. At the same time, it does not require any knowledge's from the mobile device users. On the other hand, in the latter the mobile device users within Android have own responsibilities to handle or enable the permission to access the mentioned prosperities.

Studies stated that new source of risks will be increased based on developing and introducing new components and elements within different platforms [4] [10] [14]. For that reason, mobile device attackers are employing new attack vectors as shown in figure 1 against the developed components within platforms incessantly. Application privilege separation model has been implemented and developed within iOS and Android mobile operating system. Mobile device (Smartphone's) in a great need and require protection against types of threats, an

application malicious and network attacks [1]. Then, to ensure that security is existed from user's expectation threats must be addressed at different levels [28]. As it is expected that installing applications form unauthorized market store, having third party application and connecting mobile devices to the networks will be increased the risks against mobile devices is expected to be tripled as well.

Android and iOS Smartphone devices have been infected by mobile malware; Root exploit is one of the channels that infect Android and iOS through 'rooting Android marketplace' and 'iOS jail breaking' [29]. In terms of mobile malware spreads it is arguably on both popular Smartphone devices has the same impact. However, it spreads faster on Android rather than iOS. Although, mobile malware risks are potentially higher with the iOS devices due to the existence of lack of isolation and jail breaking [10]. iOS and Android Mobile users can download application on both market places such as App Store and Google Play respectively. Meanwhile, many Android mobile users can install application from the USB devices [29].

It is worth mentioning with rapid growth of smart devices mobile threats, malwares and malicious attacks also increased. The trends and new studies showed that the possible reasons behind increasing mobile threats, malwares as well as malicious attacks are forthcoming from increasing of mobile users [21] [31]. The mobile users, developers and companies required increasing security awareness programs to improve and updating IT policy and threat modeling as shown in figure 1 for risk identification. At the same time, security risks might be doubled while the sensitive user information has been uploaded and stored on the mobile devices 'encrypted password-protected', 'strong password', 'security assessment' and 'wiped information remotely' [13]. The other recommendations are 'secure coding practices', 'view-only accesses, 'Increase monitoring controls', and 'assess threats against web-based applications and infrastructure'.

7. MANAGERIAL IMPLICATION

Due to the increasing significance of Smartphone and other mobile devices to accomplish task for consumers and works, these devices have become more attractive for attackers. Consequently, the security aspect needs to be delivered very seriously. The real security can be achieved by protecting the device, user's data as well as applications on the device. Here some main essential managerial steps to insure the mobile security:

1. Having good security awareness: educating people to operate securely such as changing their lock pin regularly, sending the errors to the IT departments whenever appeared, backing up data, and accept patched which will be provided by companies. Security awareness has become vital to achieve high level security because people are usually do not care about security and according to a survey about users attitude about privacy and security [10], roughly half of participant said either concerned or somehow concerned about mobile data security while the rest they have never thought about it. Finally, users should be learned to use latest update of software.

2. Baseline requirement in terms of corporate security policy should be in place during a planning phase of mobile device deployment may include:

    - Password protection at power-on
    - File or directory encryption
    - VPN for email and internal network access
    - On-device firewall
    - AV software
    - Latest security patches

3. Locking the devices: Locking device is crucial part of achieving security because devices can be lost or stolen. Having lock on the devices may guarantee loss of data on the devices along with platforms should have proper policies to enforce users to have long and strong passwords. In addition, enable remote wiping.

4. Providing patches: Eventually, smart phones and other devices need to be patched regularly to avoid the risks and threaten which platforms may face after releasing.

5. Installing antivirus: having good antivirus will help users as well as platform to operate securely since anti viruses can block bad applications and preventing malicious programs to access data and corrupt device itself.

6. Having back up of your data regularly, use encryption to hide valuable data from hackers and do not access non-secure wireless networks.

8. CONCLUSIONS

In conclusion, the introduction and analysis of various mobile devices and mobile application security issues by providing wider techniques of threats in mobile. The major risks as well as major threats that faced smart phones compared to the PCs have been highlighted. Furthermore, from the literature study and researcher prospective threats in data security and communication are going to become more difficult to manage because hackers are looking of different ways to breach smart device platform. This can be done through added levels of security and manufactures access points as well as application programming interfaces API's. Hence, mobile applications tackle each aspect of our life and simplified the way that apps can be used for: business, social networking, shopping, travel, education, banking and network utility. In addition, security is one of the potential and challenging activities which need to be taking into consideration during the developing phases. More importantly, developers must consider their application's levels of security within different popular platforms such as iOS and Android. It can be identified that the number of mobile end users who are downloading applications are increasing rapidly. Therefore, applying better security mechanisms should be in place during application signing. To conclude, further education for user about how to use mobile safely found to be crucial to degrade the number of data lose, attacks as well as threats.

9. REFERENCES

[1] Asokan, N., Davi, L., Dmitrienko, A., Heuser, S.,Kostiainen, K., Reshetova, E., Sadeghi, A. (2014) '*Mobile Platform Security*', Morgan & cLaypool publishers

[2] Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S. and Wolf, C. (2011) 'Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices'. *2011 IEEE Symposium on Security and Privacy.*P 96-111.

[3] Benjamin, F., Seda, G., Maritta, H., and Holger, S. (2010)'*A comparision of security requirements*

engineering methods', in requirement engineering.

[4] Bhattacharya,P.,Yang,L.,Guo,M.,Qian,K.,andYang,M.(2014), 'Learning Mobile Security with Labware', IEEE Security & Privacy

[5] Braun, P., and Rossak, W. (2005). '*Mobile agents. Basic concepts, mobility models and the tracy toolkit'*. dpunkt. verlag.

[6] Bürkle, A., Hertel, A., Müller, W. and Wieser, M. (2008) "Evaluating the security of mobile agent platforms' *Springer Science+Business Media, LLC 2008*

[7] Certic, S. (Not Given), 'The Future of Mobile Security', *CS Network Solutions Limited*, [online]. Available at: http://www.cs-networks.net [Accessed 4th September 2014].

[8] Chen, M. (Not given), *A methodology for building mobile computing applications*, USA

[9] Clarke,N. & Furnell, S. (2007). 'Advanced user authentication for mobile devices'. *Computers & Security*, vol.26, (2), pp. 109-119 [online]. Available at: http://www.sciencedirect.com.libaccess.hud.ac.uk/science/article/pii/S0167404806001428 [Accessed 7th May 2014].

[10] Delac, G. Silic, M. and Krolo, J. (2011), Emerging Security Threats for Mobile Platforms' *MIPRO 2011*, May 23-27, 2011, Opatija, Croatia

[11] Dimensional Research, (2014), The Impact of Mobile Devices on Information Security: A Survey of IT and Security Professionals, [online]. Available at: https://www.checkpoint.com/downloads/product-related/report/check-point-capsule-2014-mobile-security-survey-report.pdf [Accessed 4th October 2015].

[12] Finneran, M. (2011). 'Mobile App Development Needs A New Approach'. *Informationweek* [online]. Available at: http://www.informationweek.com/mobile/mobile-app-development-needs-a-new-approach/d/d-id/1099351?page_number=1 [Accessed 4th September 2014].

[13] Flora, H. and Chande, S. (2013). 'A review and analysis on mobile application development processes using agile methodologies', *International Journal of Research in Computer Science, eISSN 2249-8265* Volume 3 Issue 2 (2013) pp. 9-18 www.ijorcs.org, A Unit of White Globe Publications

[14] F-Secure Lab, (2013). '*Mobile Threat Report'* [online].Availableat: http://www.fsecure.com/documents/996508/1030743/Mobile_Threat_Report_Q3_2013.pdf [Accessed 4th September 2014].

[15] Gehrmann, C. and Ståhl, P. (2006) '*Mobile platform security*' Ericsson Review No. 2

[16] Geirland, J. (2002). '*The feature: mobile intelligent Agents*'.[online].Availableat:http://www.thefeature.com/article?articleid=26051 [Accessed 4th September 2014].

[17] Gupta, A., Jaiswal, B. and Tewari, C. (2013). 'Security Requirements Engineering: Analysis and Prioritization'. *In Proceedings of the International conference on Software Engineering Research and Practice*, 2013. Page 38-45, Las Vegas

[18] Healey, M. (2011). The OS Mess: 5 Ways to Take Control. *Informationweek* [online]. Available at: http://www.informationweek.com/it-leadership/the-os-mess-5-ways-to-take-control/d/d-id/1098641? [Accessed 4th September 2014].

[19] IDC.com (2015). Smartphone OS Market Share, 2015 Q2 [online]. Available at: http://www.idc.com/prodserv/smartphone-os-market-share.jsp [Accessed 4th September 2015].

[20] ITU.int, (2015), ICT Facts and Figures: The World in 2015, [online]. Available at: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx [Accessed 4th October 2015].

[21] JRivera, J. and Van der Meulen, R. (2014). 'Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013'.

[22] Luo, J. and Kang, M., (2011), "Application Lockbox for Mobile Device Security," Information Technology: New Generations (ITNG), 2011 Eighth International Conference, pp.336-341, 11-13 April 2011

[23] Mahmood. S. (2013). 'An investigation into mobile based approach for healthcare activities - Occupational Therapy System'. *In Proceedings of the International conference on Software Engineering Research and Practice*, 2013. Page 95-101, Las Vegas

[24] Mcafee (2015), "Threats Predictions", [online]. Available at: http://www.mcafee.com/es/resources/misc/infographic-threats-predictions-2015.pdf [Accessed 4th September 2014].

[25] Mike Park. (2012). 'Mobile Application Security: Who, How and Why' *Trustwave SpiderLabs*

[26] My First Mobile App – Apps World, (2014) '*Mobile application design & development trends -2013'*

[27] Petkovic, M. & Jonker, W. (Eds) (2007). *Security, Privacy, and Trust in Modern Data Management*. Verlag: Springer

[28] Potter, B. (2007). 'Mobile security risks: ever evolving'. *Network Security*, vol.2007. (8).pp. 19-20

[29] Qing L. and Greg C., (2013), Mobile Security: A Look Ahead, IEEE Security & Privacy

[30] Rowan, M. and Dehlinger, J. (2013). 'Research Trends and Open Issues in Mobile Application Software Engineering'. *In Proceedings of the International conference on Software Engineering Research and Practice*, 2013. Page 38-45, Las Vegas

[31] Scandariato, R. and Walden, J. (2012). 'Predicting vulnerableclassesinanAndroidapplication'.*InProceedingsofthe4thinternationalworshop on Security measurements and metrics*,ACM, USA, 11-16.

[32] Statista.com, (2015), Number of apps available in leading app stores as of July 2015, [online]. Available at: http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ [Accessed 4th October 2015].

[33] Veikko, I., Eija, K. & Marketta, N. (2009). 'Defining Ethical Guidelines for Ambient Intelligence Applications on a Mobile Phone'. *In: Proceedings of*

the 1st International Conference on Intelligent Environment (IE09), 20-21 July 2009, Technical University ofCatalonia, Barcelona. [online]. Available at: https://www.dora.dmu.ac.uk/handle/2086/5295 [Accessed 25th July 2014].

[34] Wang, T., Lu, K., Lu. L., Chung, S., and Lee, W. (2013). 'Jekyll on iOS: When benign apps become evil'. *In USENIX Security Symposium*, 78

[35] Yao, H., Lian, L., Fan, Y., Liang, Q., and Yan, X. (2013), 'The Evaluation of Security Algorithms on Mobile Platform', *IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*