Survey of Android Phone Security

[1]Garima Jain, [2]Mr. Ratan Singh

[1]M.Tech. Scholar, [2]HOD CSE
Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal

***ABSTRACT*: At the present time, Smart-phones and other Mobile devices have turned out to be extremely essential in every part of our life. Because they have similar capabilities as compared with desktop in addition, they proved to be powerful in terms of CPU (Central processing Unit), Storage and installing several applications. For that reason, in wireless communication technologies, security is considered as an important factor, predominantly in wireless ad-hoc networks and mobile-operating systems. Furthermore, based on augmenting the range of mobile applications contained by multiplicity of platforms, security is considered as one of the most valuable and substantial debate in terms of issues, precision, trustees and reliabilities. This paper introduces a merged report of thriving security on mobile-application dais and offering information of vital threats to the users and the enterprises. Moreover, this paper presents a variety of techniques as well as methods for security measurements, the analysis and prioritization within the zenith of mobile platforms. In addition, it increases awareness and understanding of security on mobile application platforms in order to avoid forensics, detection and countermeasures which are used by the operating-systems. Finally, this study also argues about the security wings for trendy mobile platforms and analysis for an inspection within a latest research in the field of mobile platform security.**

***Keywords*: Threats, Cyber Strategy, Mobile Platforms, Security, Security Awareness, Sensitive Data and Vulnerability.**

I. INTRODUCTION

Smart-phones and mobile devices have become incredibly vital parts of our life. Since they have provided same capabilities as well as facilities that desktop work stations provide. However, it is a big challenge as far as matter of security is concerned [22]. At the present time, malicious programs and the numbers of attackers have increased very rapidly. As per the threat-predictions report [24] 2015 will be the turning point as the threats to mobile devices in which the total number of mobile malware samples surpassed 5 million in Q3 2014. As a result, security prerequisites and concerns within various mobile platforms have become an objective for researches many studies. As a consequence, one of the most crucial decisions within the use of Smart-phones is the selection of appropriate mobile platforms. The three fundamental categories of the security goals and objectives of information in an organization are confidentiality, integrity and availability [3] [17]. More to say, security can be analysed through: _confidentiality, integrity, authentication and authorization‘[15]. Furthermore, within security of mobile platforms, risk analysis is also considered as one of the main crucial factors. In addition to these, when security issues and gaps have managed to survive, it became vital to identify the challenges against existed security issues [30]. Due to implausible increasing of memory, data transmission and processing the security incident turned out to be more powerful on mobile platforms and phone devices [2].

This paper focuses mainly on the 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 assessment of the existing methods and studies will be presented. This study introduces both generic model security architectures ‘and _threat model‘of mobile platforms within two main popular platforms of IOS and Android. The last but not the least, the security issues and privacy in mobile platforms will also be discussed.

It is worth mentioning that in this paper, security in mobile platforms has been analyzed in different perspectives in which it identifies how both IOS and Android platforms have implemented security models against threats.

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

II. THE IMPORTANCE OF THIS STUDY

Currently smart-phones and mobile devices have become the most targeted sources for hackers and malicious programmers. In accordance with the threat prediction report from McAfee Labs in Q3 2014 the total number of mobile malware samples exceeded 5 million. Additionally, about 110 million Americans— equivalent to about 50% of US adults—have had their personal data exposed in some form in the past year. So, it can be recognized as essential to have the state-of-the-art about how mobile platforms provide security mechanism. Therefore, people will have right materials, to choose the right platform in everyday use. Finally, this survey will help platform providers to ameliorate their security mechanism based on the findings of this study.

III. BACKGROUND

The size of mobile market significantly increases every year, while mobile phone user‘s subscriptions were estimated around 7,084,987 billion by 2015 based on the ITU report in [20]. To enforce application security every mobile platform has introduced and implemented their models or approaches. The three classified sections of threat model within mobile platforms are Attack goals, attack vectors and mobile malware [10] as shown in figure 1 41 Generally, the security is defined as ―the capability of a software to avoid intentional or involuntary 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 condition is one of the developing areas for the researchers to put their centre on mobile platforms due to emerging huge numbers of mobile applications within various mobile platforms. Likewise, developers are most likely to concentrate on security constraints during some of the processes (phases) within the variety of mobile application models and methodologies.

Although mobile is an instrument or a personal device which would be trustful for whom that will use the application on the mobile phone for performing various actions. One of the essential concerns of therapists or doctors is transferring the patient's sensitive information to the external servers [23] [27], [33]. Despite of that, the increase in the use of mobile applications for different aspects need an essential level of security because of the existence of availability services and sensitive information inside mobile applications [9] [28]. Additionally, there is a requirement of developing a technology which gets rid of the threats, unconstitutional entrée to the information via mobile, and avoid internal access to the stored information authentication process for mobile application.

Confidentiality, availability and integrity are considered as three main crucial requirements that each system must have to secure the data and provide the suitable security solutions. Confidentiality assures that the information will not reach to wrong destination; at the same time it must also guarantee that right people acquire 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 indecent behaviour.

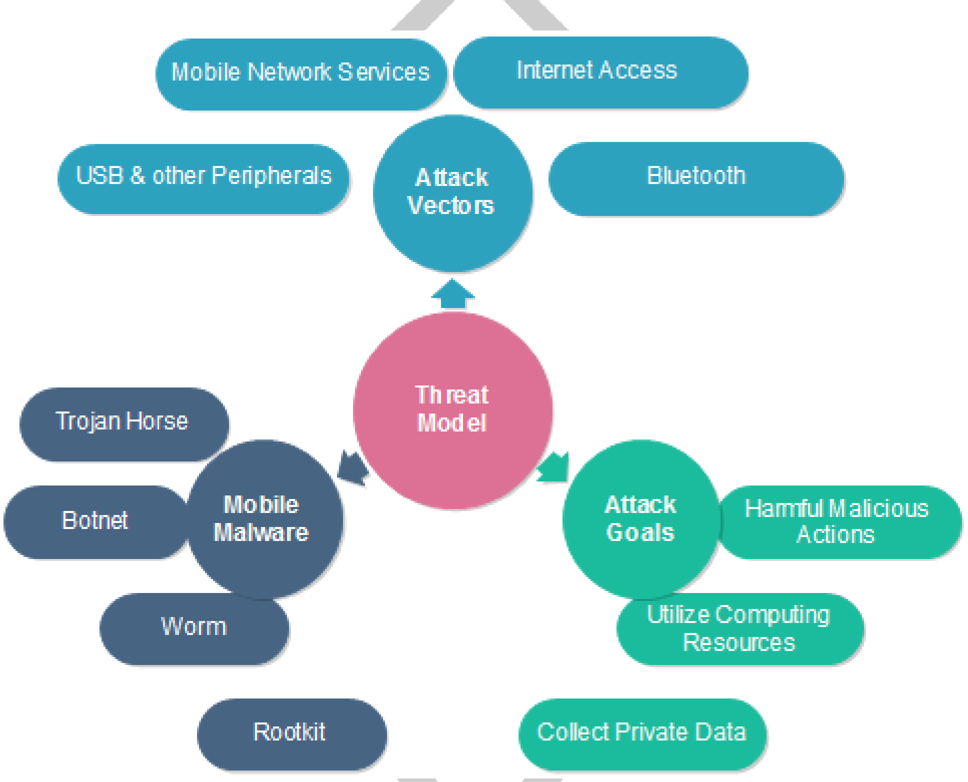


Fig 1: Mobile Platform Model Threats (MPMT) [10]

Furthermore, growing and enlargement of mobile applications and platforms, security concerns are rising in different aspects of our lives. [7]. the four fundamentals of security in mobile computing are information security, system security, network security, and physical security. In the meantime, 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 ventures are requiring limited security mechanisms from IT companies and technology infrastructures with applying new levels of security in order to safeguard user‘s data. Meanwhile, existing technologies for the security could be embedded within mobile platforms architecture such as _firewalls, authentication servers, biometrics, cryptography, and Virtual Private Network‘[8].

IV. MOBILE APPLICATION SECURITY PLATFORMS

Mobile application growth in a variety of platforms is based upon functional and non-functional requirements [17]. Currently, different types of platforms exist to organize mobile applications with dissimilar private policies. Consequently, this research focuses on the most invaluable and admired mobile application platforms in the world. Furthermore, it discusses how the security within every platform is unique and different from each others for example, Motion BlackBerry OS, Apple IOS, Google Android, and Microsoft Windows Phone. There are some very important security issues to be assessed and studied such as _battery capacity limitation‘, and encryption algorithms power consumption‘, were having major impacts on mobile devices [35].

In addition to these, taking control over third-party application is a complicating task within every mobile apps store, of which they have huge impacts on augmenting the security issues within mobile platforms. Dimensional Research institution in [11] stated that Android is being relied less whereas Windows Mobile and BlackBerry is trusted more for security‘. Meanwhile, on the basis of same survey or report most of the participants understood that the security hazards were the main causes of the mobile security platforms. A huge number of IT professionals said that Android was the riskiest 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 towards Android security issues continued to grow rapidly and 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 chief risks involved were from the unknown sources like publisher (developer) who have threatened and attacked attractive mobile platforms. Meanwhile, web-based applications were backed up by some of the well-liked mobile platforms such as Windows Phone 8, IOS, and Black Berry 10 [1]. In terms of having all the vulnerabilities[29], mobile Web browser applications are facing the similar security hazards on Web View Technology like computers _Application layer‘, Middleware layer‘ and _Kernel layer‘ and they are vital extension layers that have been recommended against privacy and security issues within different mobile platforms [1]. In addition, dissimilarities within mobile platforms, for instance, the security architectures are completely based upon a similar model; Permission-based access control, code signing, and application isolation and they are the three basic built security methods among various mobile platforms [1].

It is worth mentioning that the past mobile platform companies were chiefly focusing on developing features rather than other crucial concepts such as security. And because of that, the misuse of platform weakness, storage and binary took place [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 research papers have been published in relation with the mobile security and the consequence of malicious application on various mobile platforms. At the same time, banking applications were one of the main targeted areas for the attackers to gain financial advantages and personal data (personal information, cardholder data). Nonetheless, the attempt is based upon the attacks to breach provisional application licensing functionality and restrictive platforms [25]. The hackers are interested in getting famous and embarrassing people. The attackers final destinations are mobile platforms, malware installation, mobile botnets and Application architecture decisions based on platform [25].

4.2 Security Threats Measurement

There are some primary measures concerned with security which needs to be looked after, for technological solutions for mobile agents such as Encryption, Digital signatures and certificates, Central management of the access permissions, the communication channels of Sandbox and Secure [6]. In fact, through the revolution of mobile devices (Smartphone) the core processes and business models can be transferred. It is obvious that the most crucial sections within life cycle of application management is security. Recent study proved that one of the most concerned areas within mobile technology and mobile system is security. According to Finnegan in [13] states that the encryption involved is not supported by various mobile operating systems and its versions. In addition, SSL-based access and VPN are some of the promising solutions to avoid achieving sensitive data. Besides, in [18] in accordance with the survey 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

V. FINDING

The security model within mobile platforms or mobile-OS can be compared on the basis of traditional access control approaches, application provenance, encryption, isolation (sandboxing), and access control [4]. Furthermore, mobile malware, web- and network-based malware are known as the important types of threats within mobile security, Bhattacharya, ET. Al in [4] categorised the fundamentals of mobile security in mobile-device security and privacy, mobile-app security, mobile network and communication security. Moreover, the professionals and code reviewers implemented security mechanisms against malicious intentions within IOS applications.. Meanwhile, it makes it safe to download and install an application on the App Store. Android platform has its own process action called application isolation, in which, an application is averted to hold up with other applications [10]. It is a widely accepted fact that, there are lots of worms recently existed and affected mobile platforms for example Ikee.B is one of the examples of theft of sensitive data from jail broken iPhones [10]. Permission based security models have also been implemented within Android platform to deal with security issues as depicted in figure 2.

Other studies like Asoka ET. Al in [1] introduced Privilege-escalation attacks, detection of malevolent applications and application hardening. Based on the literature study within mobile platforms the 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.

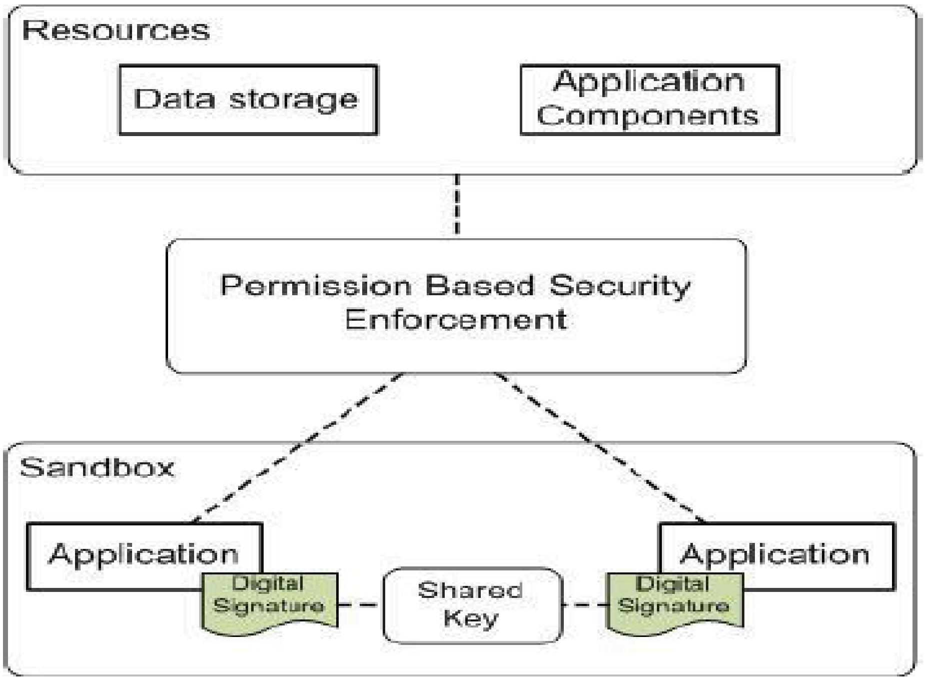
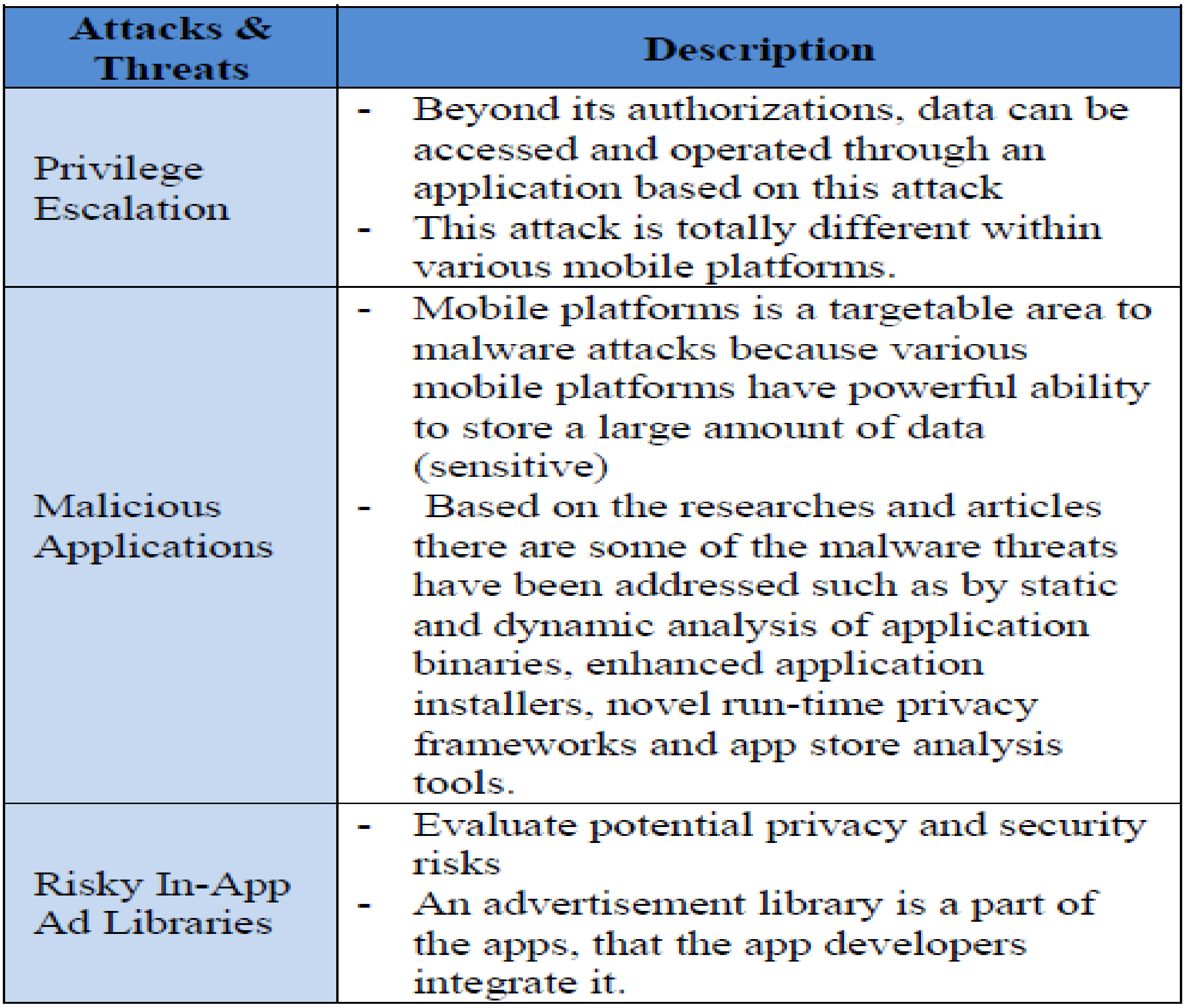


Fig 2: Android Security Model [10]



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.

Table 1. Attacks and Threats [1]

Moreover, when the mobile devices are stolen or lost the security risk is alarmed. Buffer overflow is yet again one of the vulnerabilities within an Apple‘s application besides the advantages of having vetting process (it is a process of reviewing the apple‘s application). It can be assumed that entire dedicated site work as a guideline for the developers and Objective-C in iphone programming language [1] [12]. Similarly, vetting process is not an actual solution against malicious actions due to the existence of various approaches to hide the malicious codes in applications [1] [34]. Thus, the vetting process has not been provided by the Android platforms for the developers. Similarly, there was an initiation of the guidelines for both users and developers for the security reasons by Google [12].

Unlike mobile web application, security and testing in native mobile applications are more fascinating [13], for that reason, mobile platform manufacturers are supposed to be building some secure applications/devices and a _secure process for issuing platform software‘ [15]. It is widely acknowledged that within mobile platforms a variety of critical architectural security constituents have been implemented such as _software and hardware security architecture‘. Nonetheless, the three main properties of mobile platform are performance, security and scalability, whose manufacture should concern about [6]. Bhattacharya et. al in [4] highlight that security in mobile operating system consists of ‖threats to‖, ‖attacks on‖, and defence, those features should be covering up\including: secure coding, cryptography, physical security, secure communication, and policy administration.

It is a widely known fact that mobile devices, in terms of hardware and operating system (OS), are the main targeted areas for attacking[2] [10]. Companies and individuals are sceptical of allowing an unmanageable piece of code to be loaded onto their machines and implement, which is, fundamentally, what a virus does‖ [6] [16]. According to the statistical study of the available apps, which can be downloaded 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 apps available according to the same study. While the windows phone and BlackBerry worlds have 400,000 and 130,000 apps respectively [32]. The underlying principle behind mobile threats and malicious exploits is based on having great numbers of application and expectation for movements and having a different OS for mobile phones as predicted in figure 3.

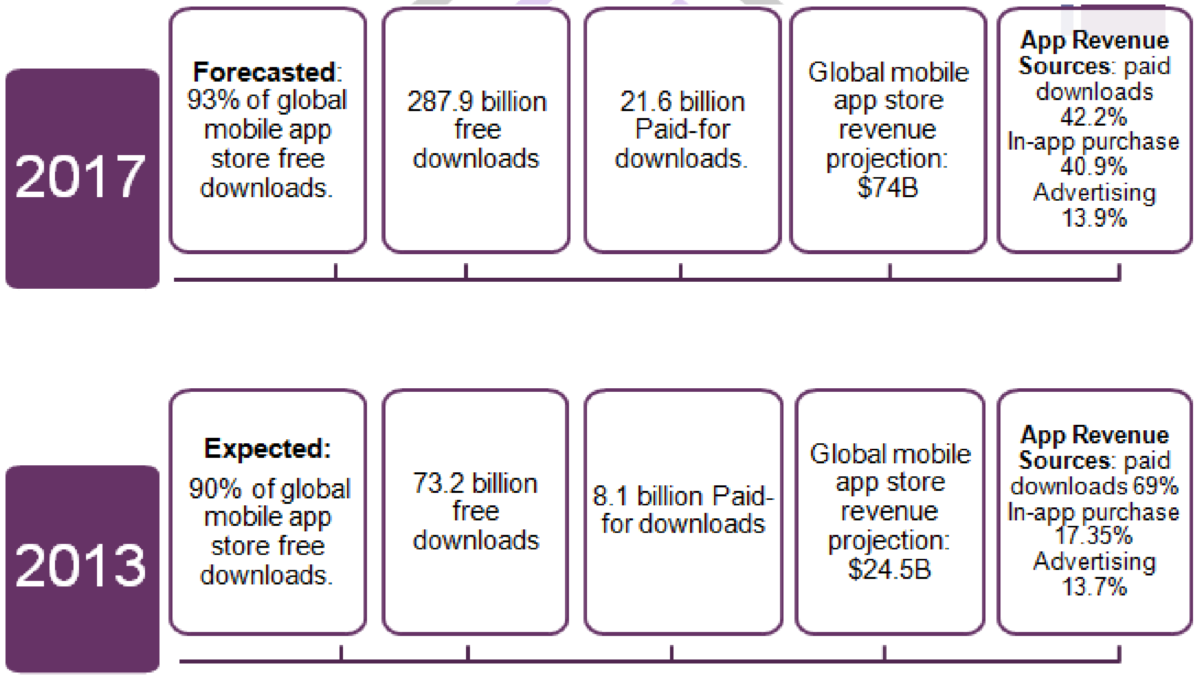

2017
Forecasted: 93% of global mobile app store free downloads.
287.9 billion free downloads
21.6 billion Paid-for downloads.
Global mobile app store revenue projection: $74B
App Revenue Sources: paid downloads 42.2% In-app purchase 40.9% Advertising 13.9%
2013
Expected: 90% of global mobile app store free downloads.
73.2 billion free downloads
8.1 billion Paid-for downloads
Global mobile app store revenue projection: $24.5B
App Revenue Sources: paid downloads 69% In-app purchase 17.35% Advertising 13.7%

Fig 3: Mobile App Store Trend adopted [26]

Potential threats could be more diverse naturally, from a different stakeholder's viewpoint. Additionally, the preliminary classes of stakeholder comprise the content provider and a secure and reliable mobile network. Necessary security must be provided by every mobile platform. The crucial security mechanisms have been clarified which include ‖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]. A secure behaviour from the mobile platforms is witnessed when the integrity of core platform software and critical data is assured. The mobile device platform must possess security functions that assure

Secure implementation and code integrity.

Today, mobile application is developing rapidly and continuously in mobile platforms. Malicious exploit attacks on hardware and OS like personal computer (PC) as well as mobile platforms threats that include Trojan horse, worm, virus and malicious application have been increasing radically [10]. For that reason, the privacy and security a smart-phone user 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 Smart-phones within different platforms, mobile users face new kinds of security issues and security concerns. All the mobile platforms must have a critical solution for the security concerns in order to attain user‘s

protection and security for their mobile devices. Unlike, Android application platform, IOS application platforms had a revision process for each new application which has to be released in application store [10].
There is diversity between the PC windows and mobile platforms such as integration within IT architecture and third party security products. In Both the aspects PC is considered as more secure as compare with mobile platforms. In order to provide secure platforms against threats many mobile platforms' infrastructures have applied several important procedures and policies such as authentication and authorization. Some researchers discussed that The key concern that is necessary to be considered against threats on mobile enterprise is allowing right user to access the devise and losing sensitive information or data stored on mobile devices [28]. Table 2 provides an overview of global Smartphone platforms sales to end-users in March 2018.

Operating System	2018	2017	2016	2015
Android	82.8%	84.8%	79.8%	69.3%
IOS	13.9%	11.6%	12.9%	16.3%
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

Table 2. Market Share Analysis [19]

As it can be seen from the above table, the Android OS is controlling the market share for years 2015, 2016, 2017, 2018 consecutively. On the other hand, IOS is taking the second place since 2015, while the other OSs is simply following. It is worth mentioning that OSs like Windows phone and Blackberry are losing the market share considerably from 2015 to 2018.

VI. EVALUATION

Unlike IOS and other platforms, Blackberry enterprise server manager has capability to apply a uniform protection policy which is impossible for Uniform security policy PIN protection and data encryption which is overridden by the users [28]. In addition, it does not permit sensitive data to be in a susceptible state. While, in the iphone and other mobile devices the data could be in danger. Authorizations are one of the decisive differences within IOS and Android platforms [10]. On the former, an application could 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 need any knowledge from the device users. En contraire, in the latter, the mobile device users within Android have their own responsibilities to handle or enable the permission to access the mentioned prosperities.
Studies have stated that new source of dangers will be increased based on developing and beginning new components and elements within different platforms [4] [10] [14]. Because mobile device attackers are employing new attack vectors as shown in figure 1 against the developed constituents within platforms relentlessly. Application privilege separation model has been implemented and developed within IOS and Android mobile OS. Mobile device is in a great need and requires protection against different types of threats and malicious network attacks [1]. Then, threats must be addressed at different levels to make sure that security exists from user's expectations [28]. Installing applications from unauthorized market store, having third party application and connecting mobile devices to the networks will increase the risks against mobile devices.
Android and IOS Smartphone devices have been spoiled by mobile malware; One of the channels is Root exploit that infects Android and IOS through _rooting Android marketplace‘and IOS jail breaking‘[29]. In terms of mobile malware spread, it is questionably, has the same impact on both popular Smartphone devices. However, it spreads faster on Android rather than IOS. Due to the existence of deficiency of isolation and jail breaking malware risks are probably higher with the IOS devices [10]. Applications can be download on both market places such as App Store and Google Play respectively by both IOS and Android Mobile users. Meanwhile, USB devices help an android user to download various types of apps [29].
It is worth mentioning that along with the rapid increase in smart devices, the mobile threats, malwares and malicious attacks have also increased. The drift and new studies mentioned that by the increasing number of mobile users it is possible that mobile threats, malwares as well as malicious attacks are forthcoming [21] [31]. The developers, companies and mobile users require increasing the security awareness programs to improve and update IT policy and threat modelling as shown in figure 1 for risk identification. At the same time, security risks might get augmented while the sensitive user data 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 examine threats against web-based applications and infrastructure‘.

VII. MANAGERIAL IMPLICATION

Smart-phones and other mobile devices have started playing a very significant role in our lives which attracted attackers. Consequently, the security aspect must be taken very seriously. The real security is protecting the device, user's data as well as applications. For insuring the mobile security some essential managerial steps are as follows:
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 they appeared, backing up the data, and accept patched which will be provided by companies. Security awareness has turned out to be a vital aspect. People usually do not care about security and according to a survey about

users attitude towards privacy and security [10], roughly half of participant said that they are either concerned or somehow concerned about mobile data security while the rest have never thought about it. Users must learn the use of latest update of software.

2. Baseline necessity in terms of corporate security policy must be in place during a planning phase of mobile device deployment. This 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 a crucial part of achieving security because there is always a danger of losing the devices. The lock on the devices guarantee the loss of data on the devices along with platforms must have proper policies to enforce users to have long and strong passwords. In addition, enable remote wiping.

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

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

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

VIII. CONCLUSIONS

In conclusion, the introduction and study of various mobile devices and mobile application must be understood. The security issues must be taken care of 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 perspective, threats in data security and communication will become harder to manage because hackers are finding different methods to breach smart device platform. Through added levels of security and manufactures access points and application programming interfaces a device can be secured. Hence, mobile applications tackle each aspect of our life and simplify the way these apps can be used, for example; business, social networking, shopping, travel, education, banking and network utilities. In addition, security is one of the potential and challenging activities which need to be taken into consideration during the phase of development. More importantly, developers must consider their application's levels of security among various popular platforms such as IOS and Android. It is of the fact that the number of mobile-end users who are downloading applications are increasing in a rapid manner. Therefore, applying healthier security mechanisms should be in place during application signing. To conclude, further education for user about how to use mobile safely is found to be crucial to disgrace the number of data loss, attacks as well as threats.

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

[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].Availablat: 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

[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 the 1stInternational 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 IJCATM : www.ijcaonline.org View publication