VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2013 ISSN(e): 2309-3978;ISSN(p): 2411-6246
Volume 1, Number 1, January-December, 2013

pp. 42-49

SECURITY ANALYSIS OF SMARTPHONE OPERATING SYSTEMS

ZEESHAN IQBAL[1], KINZA KHAN[2]
[1]Kohat University of Science and Technology
Kohat, Pakistan
zeeshan.zn@gmail.com
[2]Kohat University of Science and Technology
Kohat, Pakistan
khan_kinza19@yahoo.com

Revised August 2013

ABSTRACT. *This paper discusses the security threats and vulnerabilities in smartphone and compares the operating system on the basis of their strengths and weakness by keeping in mind the security. Our purpose is to evaluate how much protected these system are, what risks can make them vulnerable and how to make these platform more strenghtend. Our work cover four main Smartphone operating system those are android. iOS, symbiyan and blackberry and anatomize their security environment. This paper Analyze to decreases smartphone vulnerabilities, maintain secrecy, integrity and availability of smartphone basic applications. We address to explore their vulnerabilities, threats and security levels.*
Keywords: Smartphone, security, android, iOS, blackberry, symbiyan.

1. **Introduction.** Today we are living in a technical world & majority of us are using cellular phone and computer. The most famous device is smartphone which uses is increasing day to day. Beginning of this technology cell phones were used for making calls and SMS not more than this while the PDAs were used as a small portable device. Ultimately, PDAs were obtained wireless connectivity and were capable of receiving and sending e-mails. So with passage of time cellular phone added more PDAs capabilities even like computers thus result in Smartphone. Now we can say that Smartphone is an aggregation of cellular phone and PDA. It is same as computer and seems to be always connected to internet. Smartphone has a complete operating system, run software and provide interface. It provides too many facilities like browsing, touch screen system, checking email, 4G networks and GPS etc. modern Smartphone has high resolution touch screen progressively, and all application which are designed for desktop is now being redeveloped for Smartphone.

We are incoming in new modern era where everything is more intelligent than before but also insecure. The best example is our phones such as cellular phone become more efficient and PDA also replace with smartphone. Though the life is too much easy with such facilities but on the other hand it also created a anxiety for human being with aspects of security. These things effect human's behavior at some extent. Keeping an ordinary cell phone doesn't tough but to keep Smartphone have not easy. As, It contain lots of personal info like transaction, account numbers, contacts etc. Smartphone have multitude applications and with each next growing application, risks also increase and therefore security concerns are also growing. As Smartphone maintain variety of applications for users, therefore mostly applications are security sensitive such as an e-wallet, banking, smartphone as a server and third party applications. Due to this private data is unprotected. Because of some important features that build the smartphone security distinctive these are developed for single user, no login process. Here we analyze the four smartphone operating system Google's android, apple's iOS, nokia symbiyan, RIM's blackberry.

Android is an open source. Android exposed in 2007 by open handset alliances. Market share of android is 75% in October 2012. iOS is operating system for smartphone based on Unix developed by apple. Market share of iOS is 14.6% in September 2012. The Symbiyan platform was officially made available as open source code in February, 2010.Symbian was previously owned by Nokia, Ericsson, Sony Ericsson, Panasonic and Samsung, now nokia is only owner of symbiyan. In 2008 nokia announced to acquire symbiyan.

Statistic signifying the usage of smartphone. Neilson reported in December 2010, 31percent of mobile users have smartphone in US. According to estimation of researcher Morgan Stanley the usage of smartphone is go over PC's in 2012.

Figure 1 shows the market share of the popular brands in 2012. Android is with first position with 59% of market share, iOS is with 23%, symbiyan is with 6.80% and blackberry is with 6.40% and others are 4.80%.

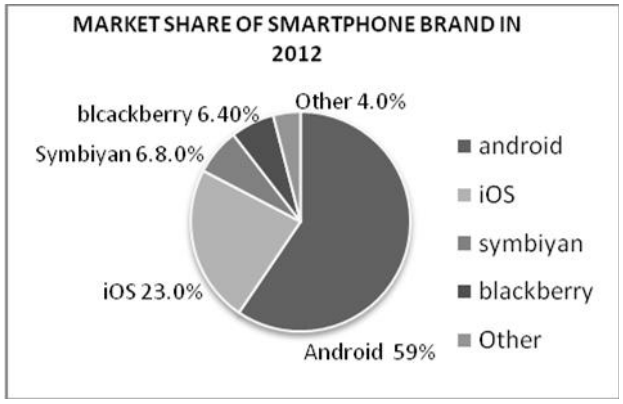

Figure 1. Market share of smart phones in 2012

2. **Related Work**. In this paper, we will review the risk involved in most emerged technology i.e. smart phones. Smart phones have become the most vital part increasing the dependency in our life. With its ease also increase the risk involves in it. The popularity of smart phones extended beyond business users with the release of Apple's iPhone and later devices running Android, BlackBerry, Windows Mobile and Windows Phone 7 operating systems. Emerging features beyond just email and web browsing; mobile devices are working well in the field of photography, running various 3rd party applications, very rich graphic version games, showing website with features of JavaScript and Flash, connecting with other mobile devices wireless, establishing private networks, acting as hotspot for other devices as well. This exponential growth has also gain the attention of hackers [1].There were more attacks on mobile devices in 2010 as more people used them for mobile computing and Web surfing [2]. User seems to be less aware of the security threats in mobile devices especially the android customers were the main targets of the hacker community. Apples framework of being able to run in a single directory and lesser user grants was the main reason behind less target area [3]. Mostly the attacks were the legitimate apps in various apps store of the mobile giants.

There were 163 known vulnerabilities in mobile operating systems in 2010, up 42 percent compared to 115 in 2009[2]. Most of the security flaws in Android smart phones were exploited by installing the harmful software. Analyzing the attacks on mobile platforms with the other cyber crimes, increase can be seen in mobile platform with the coming year onwards. The security architecture of Symbiyan OS v9 is relevant to all security practitioners and will influence the decisions made by every developer that uses Symbiyan OS in the creation of devices or add–on applications. Symbiyan OS Platform Security covers the essential concepts and presents the security features with accompanying code examples [3]. Windows 8 Safe Boot feature will increase the security level to load any malware or any other Trojans to provide the digital signature to authenticate to operating system. This feature will also increase the interest level of hacker to unlock it and use it legitimately. Safe Boot Feature means that custom ROMs will be near impossible to curate due to the lack of access to the correct digital signatures [4]. The security mostly depends on the user. One of the major threats in Smartphone is by physical attack. To make security sure user should be a smart. Physical attacks are executable by irresponsibility of users [5] Trojans were found in Symbiyan which overwrites application, cannot run antivirus automatically change system file due to which phone is not recharged [6]. Cabir virus was designed in June 2004 by expert writers 29A.[6] In April 2011 Apple restructured safari browser and to

getting this updated version, Apple issue a SSL certificate but those were fake and through which local area information might be hack. Even it is said Smartphone is vulnerable as a server and an e-wallet. As s server established a connection between devices, user does not know about risk of applications that run on server side. As an e-wallet the private information related to transaction, E-ID is also highlighted [7]. Unauthorized users crack security. It can take advantage of computer files system if it is not password protected or encrypted [8]. Blackberry is affected by newly unreported malware. [9]

3. **SECURITY.** With the passage of time Usage of Smartphone is increasing and therefore the concern of hackers towards it is also increases. Smartphone should be secured like other devices as it is also an information system. Here we give an overview of popular brand of operating system these are android, iOS, symbiyan, and blackberry. Every system contain Trusted Computing Platform(TCB), trusting computing environment, process capabilities, data confinement, install time, runtime and file sharing.

3.1. **ANDROID.** The more target operating system is android because of its open source distinctiveness. Android is Linux based operating system and programmed with java. Meanwhile some changes are made in kernel by Google. Memory, process and drivers are managed by kernel. The TCB uses some Linux security method for example every application runs under a isolated POSIX (Portable operating system interface) user ID, resource allocate to user process. However, android is open source but Linux is extremely confined and cannot be change. In trusting computing environment there is kernel and kernel consist of layers. 1st layer contains basic C-libraries, SQL database engine it provide storage of data. 2D and 3D graphics library, 2nd layer consist of virtual machine. Android runtime is controlled by Dalvik virtual machine and core libraries. Framework of is the key element through which application frankly cooperate with. Manage call services and resource management Next layer contain the lifecycles applications. Main mechanism and a few system processes run with root privileges, and there is no access control method for system process. Signature checking Permission is approved at install time. Android have four types of permission set signature, system, normal, dangerous [9]. Signature and system are not available for third party while normal type of permission is by design fixed for application without the involvement of user while dangerous permission are require at install time[9].Some applications need user authentication and while some runs automatically through adb install attribute. User cannot request more permission at run time as each application has its own user ID. Each application runs under virtual machine. Sandbox runs in their own memory.
Due to open source nature of android the most potential threat is third party applications. Google assign the responsibility to the users. It promote all types of malicious applications and user attracts towards latest uploads which are distrustful. For example weather app created by the researchers Derek Brown and Daniel Tijerina to check the possible effect; it assembles user data like GPS coordinates and phone numbers. After the 24 hours of releasing the app the researcher caught 1,864 phone cables. To maintain security halt automatic sharing of Bluetooth and also keep turned off when it is not in use. [10] If using interface which doesn't ask for permission to user then it possibly risky.

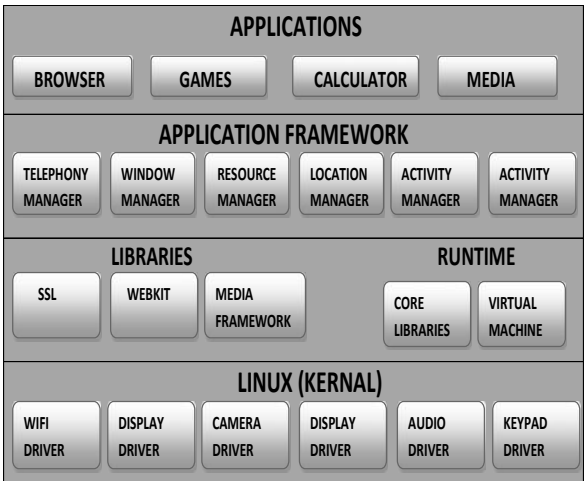

Figure 2. Proposed Android Framework

3.2. **iOS.** Apple considered the security of iOS platform at basic level. iPhone, iPod, iPod touch uses iOS operating system. iOS is derived from Mac Drawing operating system. The operating system deal with hardware devices and provide mechanism necessary to run native apps. iOS structure contains Software Development Kit SDK. The native apps of iOS are developed by the iOS SDK. It is also a layered architecture. 1st layer is application layer, the user interactive. iOS has XNU kernel and derived from UNIX and OS X operating system. It is programmed with objective C, C, C++.iOS and O SX has mostly same framework. The main difference between these is user Interface. So we can import app from OS X to iOS. The core libraries have coded same as OS X Mac operating system. Next cocoa layer provide framework to manufacture iOS application. It maintains features such as high level services, touch-system input and many more [11]. Media layer make available rich graphics, audio and video services. Low level layer is core OS it sustain system utilizes etc. user cannot communicate with it directly. iOS uses Mandatory Access Controls (MAC) mechanism and sandboxed for restricting the potential of applications. Application are isolated from each other in sandbox, one malicious app cannot harm to another. Application should ask from users what kind of services they are using. Those apps using the services should be granted a popup messages by which a user can accept or reject the permissions. By doing this a user will be more confident on the app. Only apple signed application are used in it. Usually sandboxes are used at attainment of resource time. Application is downloaded from app stores. Every app is run in its own directory and is recognized as a User ID.
Instead of too much confined system iOS has also effect by viruses. Such as in April 2011 Apple issue security certificate associated with safari browser but they were fake certificates where someone was hacking personnel information of user. The more attentive threats come in iOS from jail breaking. Why do user do jail breaking? Because user need complete access of iOS operating system. Users install themes and games without apple authorization. The first jailbreak was in July 2007 after the month of released.

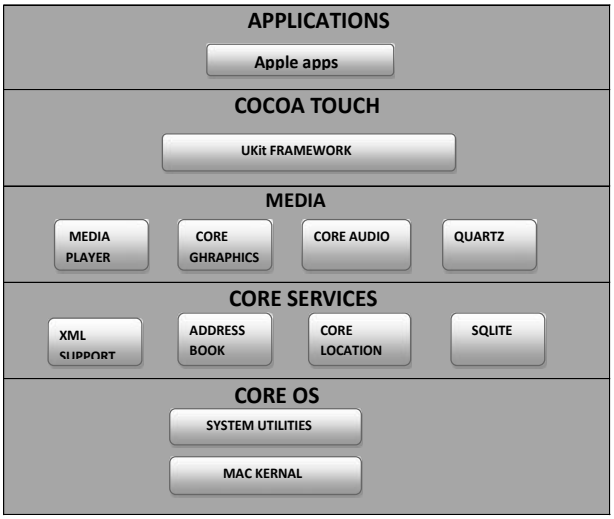

Figure 3. Proposed iOS Framework

3.3. **SYMBIAN.** Symbian operating system exists since about 2001. The Symbian operating system became fully open sourced in February 2010 which opens more risks for application developers to understand and consider security requirements. Symbian OS consists of its own kernel, file system and software installer. Since starting symbiyan has EPOC kernel which ran several operating systems. That was written in assembly language. However that system was not fully secure from malicious code. After few years Pison released new architecture which was based on C++ [14].In 2004 this EPOC kernel was replaced with EPOC2 and now current kernel is EKA2 which setup real-time warranty [14]. Trusted computing base (TCB) of symbiyan has three components kernel, software installer and file server. Trusted computing environment (TCE) run with different privileges. Symbian supports execution of add-on applications. Digital signatures of the applications are checked. If a signed application wants to use some service, it must request that TCE run the service on its behalf. TCE will only accept the request if the application has been granted that much privileges. Unsigned applications can only perform some operations that do not require privileges. Process only access specific

parts of the file system, all of the users' private data can be kept protected and parted from the applications processes. Symbian software installer ensures that add-on native software is installed on the mobile phone with the correct set of security features. It handles the installation of the software directly running on Symbian OS, not on a Java Virtual Machine. The complexity of Symbian OS programming might distract malware writers looking for fast results. Third-party application checking is a good method for malware prevention.
Three types of Trojans were found in symbiyan

1) Trojan.SymbOS.Dampig: Which overwrites application.
2) Trojan.SymbOS.Drever: Cannot run antivirus automatically
3) Trojan.SymbOS.Fontal: change system file due to which phone is not revived

Cabir virus was designed in June 2004 by expert writers 29A [6].

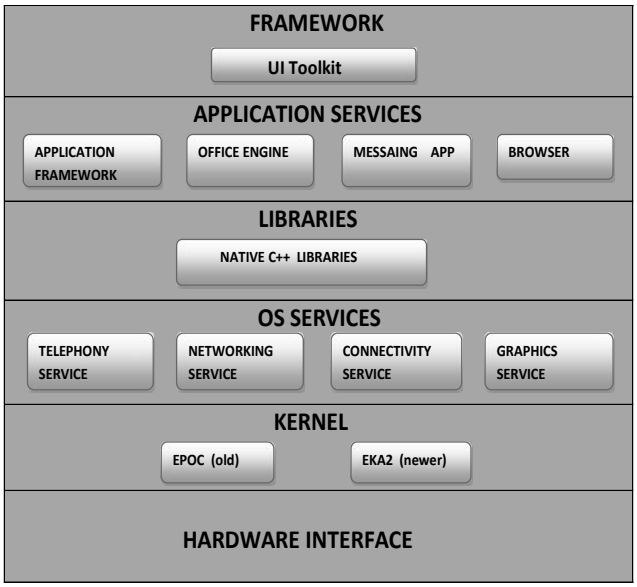

Figure 4. Proposed Symbian Framework

3.4. **Blackberry.** Blackberry was released by RIM(research in motion).In the beginning Blackberry focus on just business companies that's why it only consider e-mail and other wireless services, later in the 5000 and 6000 series blackberry has switch to mobile phone and initiate kernel. BlackBerry OS has a Java based kernel, and uses an ARM architecture. RIM designed architecture in two types of mode BIS and BES. BIS (Blackberry Internet Service) is manufactured for normal user and BES (Blackberry Enterprise Solution) is for business purpose [5]. Yet BB does not have its own processor it uses Intel XScale processor. The memory segment is divided in three parts memory card an voluntary memory, application memory reserve for apps, device memory is for files and other multimedia features. The default method of authentication is user password. Blackberry support digits and characters both. The information stored in blackberry is totally encrypted therefore it considered more secure. Third party developed authentication system also exists. Blackberry operating system doesn't require RIM signed applications. The platform's security model applies restrictions to third party applications demanding to access protected API's by demanding the signing of the application with a cryptographic key provided by RIM. This process provides poor source origin and code integrity, without providing any guarantee about the legitimacy and/or the security level of the third party application. Though RIM does not examine the third party application that running on blackberry but to keep as a precautionary measure it does control the API's, classes or methods to avoid any risk [12]. RIM provides store for applications named Blackberry App worlds.In Blackberry boot loader is used to check whether the operating system has valid signature or not. Third party applications run in a Java Virtual Machine. For current versions of blackberry, there is no known way to root the devices. They are safe from rooting or jailbreaking. Blackberry uses sandboxing that encapsulates all running processes. Every process has its own space in memory with restricted permissions. Every running application can only access data of

its own directory. Blackberry OS has some applications which just check the checksum of installation package whether it is previously reported malware or not. This cannot check the newly created malware and thus is not enough to protect the device from malware. The reason of blackberry popularity is efficient service of sending or receiving e-mail. Blackberry has most reliable email. It holds up the feature of office application. Blackberry uses their own servers so they are very secure.Source code of blackberry are not open neither RIM gives remarks.

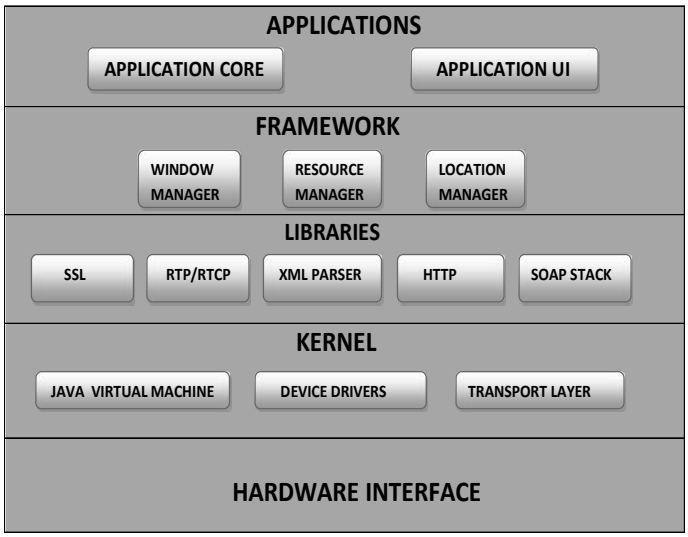

Figure 5. Proposed Blackberry Framework

4. **Threats And Vulnerabilities**Threats are can be anything or a person which possibly spoil the system. Vulnerabilities are the weakness and flaw in system.

MALWARE. One of the most known security threats to open mobile phones is malware. Trojans (malicious programs which pretense as nonthreatening ones), worms (malicious programs which send copies of themselves to other devices) and viruses (malicious code which attaches itself to authentic files and is carried along with them).
Malware targeting Symbiyan OS started to appear in June 2004. In the case of symbiyan smartphone private data is accessible by applications of any trust level while in Android smartphone, self-signed applications can be installed which can cause users to install less tested applications on their devices. Symbiyan was also affected by the Trojans that seemed to be harmless but when installed, the corrupt the configuration settings and made applications stop working. A malware affected mobile phones running Symbian OS. It can send messages to phone numbers. It also can download and install another malware. However none of the malware evaded the symbiyan OS software install security controls.
Blackberry is most secure operating system. Blackberry has strong encryption software. However installing third party apps can be vulnerable as it is not examined by for malicious behavior and Black-Berry does not operate a remote application deletion mechanism.

SECURITY CODE. Our own self is our bad opponent if we never keep our device password protected. More data is leak through this action when there is no security code. An authorize user can access data. It can be alter whole system.

WEB LINKS. Another threat which can greatly damage the smartphone security is hidden web links. In smartphone user can't read the URL before clicking it while this problem is very rare with PC's users.

UNTRUSTED APPS. This is mostly influenced in android OS because it runs every app. Hackers have created many malicious apps. It may pretend to be real app but actually it's fake. These fake apps might be asked for login approval user password or username.

FAKE SMS. It is unbelievable but it really can happen hackers send fake SMS contain link or any other malicious code via this hacker hacked all information of the users. Malicious party has been affecting Smartphone with first-class text messages; users are unaware of these until they didn't receive their monthly bills. As reported that certificates are issue by financial institution and banking when user downloaded these certificate it had ability to seize all info about account password or other information [13].Same report in Federal prosecutors in New Jersey inspect several Smartphone illegally spread information about their users [13].

PHISICAL ATTACK. Having physical access to data. Device stolen, modified hardware, installing malicious app. For example person left his/her mobile somewhere and attacker replace it battery with fake one having microphone on it if when user made call the attacker eavesdrop on this person[5].

FINANACIAL ATTACK. This is also a main category of threat. Hackers made expensive calls from hack device and user came to know when they paid monthly bills. On the other hand they might buy expensive devices pretended to be real user.

UNSECURE Wi-Fi CONNECTIONS. If we are connecting through public wifi hotspot our system must be at risk. The user who have unauthorized wifi connection whether it is intentionally or unintentionally having victims of an attack. It is easy to captured data by eavesdropping over wi-fi. Sometime public devices might be set as a hotspot hackers may possibly installed key logger to capture all keystroke our password can be hack, can access our browser history. For private use i.e. in homes make sure router has password protected.

PERIPHERAL DEVICES. Users connect their device unconsciously to any other device and consider it less vulnerable.

JAILBREAKING. Jailbreaking is one of the most sensitive action. When jailbreaking occur it can run any software without the permission from a company. Whereas jailbreaking is not an illegal act.

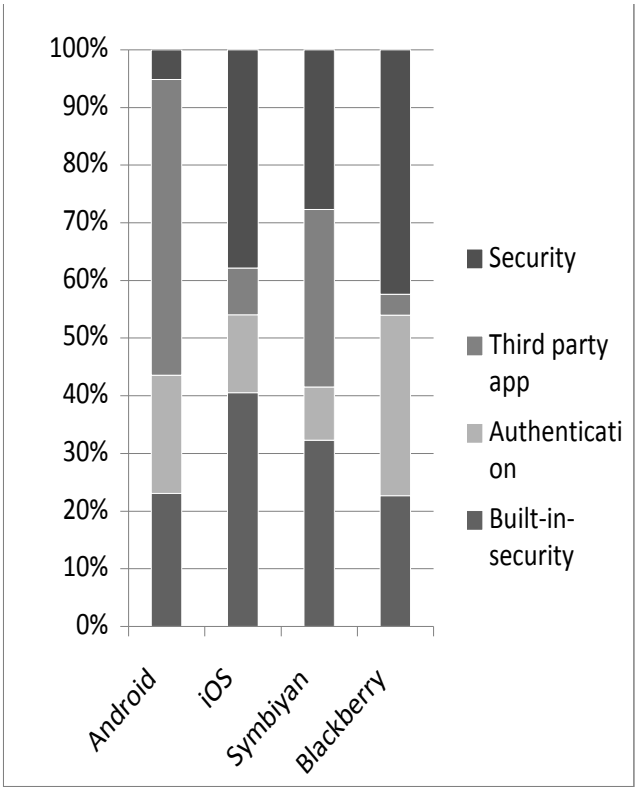

Figure 6. Smartphone operating system with resect to security

5. CONCLUSION:

100% security is impossible for any operating system. Any how we can gain much security to keep precautionary measures. Combining the different feature more operating system to one might be the best suitable choice for securing the operating system. Make simple architecture but protected. Disable all functions when they are not in use. Be sure when corresponding with other program is it trustful or not. Security of Smartphone should be at an abstract level. Where basic concern will be least privileges, permission are granted by developers and users.

REFERENCES

[1] Ernst & Young. (2012). Mobile device security - Understanding vulnerabilities and managing risks, Insights on governance, risk and compliance.

[2] F. Y. Rashid (2010), Symantec Reports Targeted Threats, Mobile Attacks increased in 2010. Retrieved July 2012 from http://www.eweek.com/c/a/Security/Symantec-ReportsTargeted-Threats-Mobile-Attacks-Increased-in-2010-191684.

[3] Programming4us (2011). Mobile Application Security : The Apple iPhone - Permissions and User Controls, Retrieved July 2012, from http://programming4.us/mobile/1750.aspx.

[4] Craig Health (2011). Symbian OS Platform Security. Retrieved July 2012, from http://www.developer.nokia.com/Community/Wiki/Symbian_OS_Platform_Security.

[5] Fredrik H (2011). System Integrity for Smartphones. A security evaluation of iOS and BlackBerry OS. Retrieved July 2012, from www.diva-portal.org/smash/get/diva2:439481/FULLTEXT01.pdf

[6] Wajeb Gharibi (2012). Symbian `vulnerability' and Mobile Threats. International Journal of Computer Science and Information Security (IJCSIS), Vol. 9, No. 10.

[7] Ishita Verma (2011). Security Analysis of Smartphone. Retrieved July 2012 from https://scholarworks.iupui.edu/bitstream/handle/18052630/Purdue_MastersThesis_Ishita_Verma.pdf?sequence=2

[8] William Stallings (2010). Cryptography and network security: principles and practice. Prentice Hall Press.

[9] Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, Phillipa Gill and David Lie (2011). A Look at SmartPhone Permission Models. In Proceedings of the 1st ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices. pp:63-67.

[10] Kadra Alvaro (2010). Android Security: Investigating Google's Mobile OS. Retrieved August 2012 from *shchu*.twgg.org/cce/ppt/Android%20security.ppt

[11] iOS Developer Library (2011). iOS Technology Overview: Retrieved August 2012 from https://developer.apple.com/library/ios/documentation/miscellaneous/conceptual/iphoneostechoverview/Introduction/Introduction.html.

[12] BlackBerry Enterprise Server: Defying the Threat of Mobile Malware. Retrieved March 2012 from us.blackberry.com/ataglance/security/1-82718_RIM_Malware_BR0.pdf

[13] Android-App-Market.com (2012). Android Architecture – The Key Concepts of Android OS, Retrieved August 2012 from http://www.android-app-market.com/android-architecture.html

[14] David Chisnall (2010). Inside the Symbian Kernel. Retrieved March 2012 from http://www.informit.com/articles/article.aspx?p=1578523.