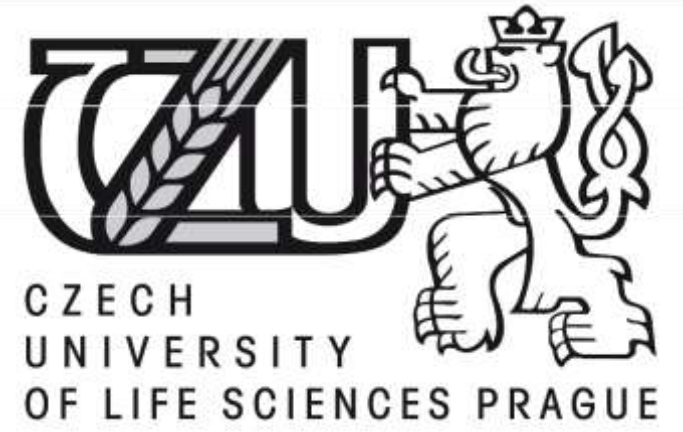
Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technology



Bachelor Thesis

OS Android

Molapo Elliot Mota

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Department of Information Technologies

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Mota Molapo Elliot

Informatics

Thesis title

OS Android

Objectives of thesis

Main goal of the thesis is to do research about security threats in Android operating system on mobile platform.

Partial goals are:

- To make comprehensive overview of current mobile platforms and their security threats,
- To identify main current security threats on Android platform and
- To investigate ways and technigues to improve the security in a given case.

Methodology

Methodology is based on the analysis of data about Android operating system. Data is obtained from the literature and also secondary sources.

The practical part will be based on the analysis of data obtained from the users of the Android operating system including the security issues experience by users or any possible faults of the system. Based on theoretical knowledge and outcomes of practical part the final conclusion will be formulated.

Schedule for processing

1) Preparation and study of specialized information resources, refinement of partial goals and selection of work process: 04 - 06/2013

2) Processing of literature overview according to information resources: 07 - 10/2013

3) Development of the own solution, discussion and evaluation of results: 11/2013 - 01/2014

4)Creation of the final document of the thesis: 02- 03/2014

5)Submission of thesis and abstract: 03/2014

The proposed extent of the thesis

30 - 40 pages

Keywords

Operating system, mobile phone, Android, security threats, Linux platform.

Recommended information sources

FOX, Richard. Information technology: an introduction for today's digital world. Boca Raton, FL: CRC Press. ISBN 14-665-6828-3.

ABHISHEK DUBEY, Anmol Misra. Android security: attacks and defenses. Boca Raton, Fla: CRC Press. ISBN 14-398-9646-1.

HOOG, Andrew. Android forensics: investigation, analysis, and mobile security for Google Android. Amsterdam: Elsevier, c2011, xix, 372 s. ISBN 978-1-59749-651-3.

Information technology business. Atlanta : NewsRX. ISSN 1945-869X.

The Bachelor Thesis Supervisor

Ulman Miloš, Ing., Ph.D.

Last date for the submission

March 2014

Electronic apporoval: January 29, 2014

doc. Ing. Zdeněk Havlíček, CSc.

Head of the Department

Electronic apporoval: March 4, 2014

Ing. Martin Pelikán, Ph.D.

Dean

Declaration

I declare that I have worked on this thesis titled “OS Android” on my own and I have used only the sources listed at the end of the thesis. As the sole author of the bachelor thesis, I declare that the thesis does not break or infringe any copyrights of any kind.

In Prague on 16.03.2014

Molapo Elliot Mota

Acknowledgement

I would like to thank Ing. Milos Ulman, Ph.D for his supervision and all the help he provided me with throughout the writing of this work. I would also like thank all the experts who provided me with their knowledge for the analytical part of the thesis and all those who took part in the survey.

OS ANDROID

Souhrn

Tato práce se zabývá operačním systémem Android. Cílem této práce je provést základní výzkum struktury operačního systému Android, jako plně funkční mobilní platformy softwaru a základní architektury své bezpečnosti. Práce ukazuje jak základní uspořádání linuxového jádra 2.6 nebo jeho aktualizace a jeho robustní konstrukce zůstává nejdůležitějším aspektem bezpečnostní architektury Android OS. Práce se dále zabývá historií vývoje operačního systému Android. Autor se snažil ukázat všechny různé verze nebo aktualizace OS Android od počátku jejich vývoje až do nejnovějších dostupných verzí.

Vzhledem k tomu, že operační systém Android je v současné době nejpoužívanější mobilní softwarovou platformou, autor práce zjistil, že je hodný dostatečný důvod k provedení tohoto výzkumu.

Autor se proto bude snažit více se zaměřit na některé bezpečnostní problémy, které takový populární systém může uložit na koncové uživatele a objevit některé z existujících chyb nebo bezpečnostních chyb, jak je uvedeno koncovými uživateli prostřednictvím výsledků krátkého formulovaného průzkumu.

Zahrnuté v této diplomové práci je také krátké porovnání operačního systému Android s Apple iOS.

Klíčová slova: Android OS, Linux kernel, smartphone, Apple iOS, Windows phone, metoda MCD, podíl na trhu, Open Handset Alliance, Android Open Source Project, bezpečnostní model Linux, bezpečnostní hrozby, Malware, Google play store.

Summary

This thesis deals with Android operating system. The aim of this work is to conduct a basic research of the structure of Android operating system as fully functional mobile platform software and the basic architecture of its security. The work shows how the fundamental layout of Linux kernel 2.6 or its updates, and its robust structure remains the most important aspect of Android OS security architecture. The work in this thesis further deals with the history of Android operating system development.

The author tried to show all the various versions or updates of Android OS since the beginning of their development until the latest available versions.

Due to the fact that Android operating system is currently the most used mobile platform software, the author of the thesis found it a worthy enough reason to carry out this research.

The author will therefore try to focus more on some security issues that such a popular system might impose on the end users and discover some of the existing bugs or security faults as reported by end users through the results of a short formulated survey.

Included in this thesis is also short comparison of Android operating system with the Apple iOS.

Keywords: Android OS, Linux kernel, smartphone, Apple iOS, Windows phone, MCD method, market share, Open Handset Alliance, Android Open Source Project, Linux security model, security threats, Malware, Google play store.

Contents

1 INTRODUCTION

This thesis is about Android Operating System, its architecture and also looks into the security threats of such an OS on a mobile platform.

The author tried to highlight the basic structure of the Android OS and how this operating system compares with other well know OS such as apple iOS. The comparison with iOS was only a short, the thesis rather look into Android OS in more detail.

In the second part of the thesis the author tried to investigate some of the different versions or developments of the Android OS on mobile platform, including some of the most popular smartphones companies that incorporated these different versions into their smartphone manufacturing.

The thesis also includes the analysis of a survey that was carried out to determine how often it is for users to catch a malware or an unintended program running on a smartphone when a user tries to download a specific app on Google's play store or anywhere else on mobile internet. This section of the thesis makes the analytical part, through the analysis of the obtained results from a short formulated survey.

The author also tried to look at the history of the Android OS and some of its alliances, such as the Open Handset Alliance (OHA) and Android Open Source Project (AOSP).

2 Objectives and Methodology of the thesis

2.1 Objectives

The main objective of the thesis is to conduct a research about the security threats on an Android operating system mobile platform.

Partial goals of the thesis are:

To make a comprehensive overview of the current mobile platforms and their security threats. In this part the author tried to make a comparison between different and well known mobile platforms and how such operating systems deal with the issue of security.

To identify the main and current security threats strictly on an Android platform handsets.

To investigate the ways and techniques to improve the security of a mobile platform is a given case. In this part the author tried to download apps on Google play store and kept record of how long it would take to run and unwanted app on the smartphone.

2.2 Methodology

Methodology is based on the analysis of data about Android operating system. Data is obtained from the literature and also from the secondary sources. It will contain knowledge from books, articles and journals. In this section the author always tried to use the latest and most appropriate literature sources.

The practical part will based in the analysis of the data obtained from the users of the Android operating system including the security issues experienced by the users or any other well documented security holes or faults of the system. Based on the theoretical knowledge and outcomes of the practical part the final conclusion will be formulated.

3 LITERATURE REVIEW

3.1 History of Android

For over thirty years, companies have invested significant resources, time and money into research and development of handheld computing devices, i.e. mobile phones and smartphones, in hope that they would open new markets. *As with traditional computers, the hardware components central to building such devices have advanced significantly and now provide a small, though powerful, mobile platform for handheld computers*. (Hoog, 2011)

The main person who we can associate with the development of Android is Andy Rubin whose past employers include robotics firms, Apple, WebTV, and Danger Inc. For his previous work for a company called, Danger Inc., he developed a smartphone and support OS most recognized from the T-Mobile Sidekick. He called the operating system DangerOS and it was built using Java. It provided a software development kit (SDK) and it included some of the features found in current smartphones we use today. Rubin left Danger Inc. in 2004 full of ideas that he maybe wanted to pursue individually. He again returned to smartphone development and teamed with several

engineers from past companies that he had worked for. Rubin formed a company in 2003 called Android, Inc.

His team began development of smartphone operating system, and Rubin was simultaneously actively involved in the marketing of Android to both potential investors and wireless carriers. He spoke with several companies over the course of time including Google, who eventually acquired Android in July 2005.

The acquisition, combined with new patents and services involving mobile and a large bid for wireless spectrum, initiated significant speculation that Google was developing their own smartphone and possibly was aiming to be a complete wireless carrier. (Hoog, 2011)

In the following weeks, Google released an early look at the Android software development kit for developers. *This allowed Google to create the first Android Developer Challenge, which ran from January 2008 through April 2008. Google set Android platform 3 aside $1,000,000 to reward the most innovative Android apps*. (Hoog, 2011)

It was later in August 2008, that Google finally announced the availability of the Android Market (currently called Android play store), where developers could upload their apps for mobile device owners to browse and install.

The initial release of Android Market did not support paid application (apps). The feature was however added in the beginning of the year 2009.

Finally, October 2008 marked both the official release of the Android Open Source Project (AOSP) and the very first publicly available Android smartphone, which was the T-Mobile G1. (Hoog, 2011)

In conclusion, it can be said that Andy Rubin is the founder of Android, since he is the man who first started and formed the company Android Inc. which later collaborated with Google and which resulted in the eventual takeover of Android Inc. by Google.

3.2 ARCHITECTURE OF ANDROID OS

Android is an open source mobile platform based primarily on the Linux 2.6 kernel and managed by the Open Handset Alliance, which consists of a group of carriers, mobile device and component manufactures, and software vendors.

The Android platform is built in most cases like any other mobile platform i.e. as a stack with various layers running on top of each other. This normally means the lower-level layers provide services to upper-level services.

The figure below shows all the layers of Android OS and their respective components:

Figure 1: Android Architecture

Source (Burnette, 2014)

In order to understand how Android is built into a fully-functional system, we examine briefly at each of the primary layers in the Android system.

From the picture above, is it quite clear that Android operating system consists of four main layers:

- Linux Kernel
- Libraries and Android Runtime
- Application Framework
- Application

All the four layers are fully examined in the paragraphs below.

At the very bottom is the kernel, Linux 2.6. The **Linux kernel** is responsible for most of the things that are usually part of the operating system kernel, and this is mostly for hardware abstraction. This is the layer responsible for all of the device-specific hardware drivers to run, enabling hardware vendors to develop drivers in a familiar environment. The bottom layer also controls some of the most basic separation between apps. (Six, 2012)

The next layer on top of the kernel is the **native libraries**. These are modules of code that are compiled down to native machine code for the device and provide some of the common services that are available for apps and other programs. (Six, 2012)

Included in the native libraries are the *Surface Manager* (responsible for graphics), 2D and 3D graphics libraries, *Web Kit* (the web engine that supports the default browser), and *SQLite* (the data store technology for the Android platform). The native libraries run as processes within the Linux kernel.

The *app runtime* also run as processes within the Linux kernel. Each app runs in its own instance of the Android runtime, and the core of each instance is a **Dalvik Virtual Machine** (VM). The Dalvik VM is a mobile-optimized virtual machine, designed to run fast on the devices that Android targets. Also present at this layer, and in each app's runtime, are the Android core libraries, such as the Android class libraries, I/O, and other similar things.

The next top layer up in the stack is the **application framework**. This is the layer where we can find compiled code running on Dalvik virtual machines that provides services to multiple apps. Also running at this level are entities such as the Package

Manager, responsible for managing apps on the phone, and the Activity Manager, which is responsible for loading Activities and managing the Activity stack**.** (Six, 2012)

Finally, apps run at the top layer, the **application layer**. This includes apps that are written by a developer, and those that Google and other Android developers do as well. *Usually, apps running at this layer include one or more of four different types of components: Activities, Broadcast Receivers, Services, and Content Providers*. (Six, 2012)

The following paragraphs give further clarification of the Android OS architecture from other sources and literatures:

Linux Kernel

The basic and first layer is the Linux kernel. The whole Android OS is built on top of the Linux 2.6 Kernel with some further architectural changes made by Google. It is this Linux that interacts with the hardware and contains all the essential hardware drivers. Drivers are programs that control and communicate with the hardware. As an example, we can consider the Bluetooth function. Most devices have Bluetooth hardware in it. Therefore the kernel must include a Bluetooth driver to communicate with the Bluetooth hardware. *The Linux kernel also acts as an abstraction layer between the hardware and other software layers*. Android uses the Linux for all its core functionality such as Memory management, process management, networking, security settings and many others. As Android is built on a most popular and tested foundation, it made the connection of Android to a variety of hardware, a relatively easy and fast task. (Android-App-Market.com, 2013)

Libraries:

The next layer is the Android's native libraries. It is this layer that enables the device to handle different types of data. These libraries are written in c or c++ programming languages and are specific for a particular hardware in case.

Some of the important native libraries include the following:

Surface Manager: *It is used for compositing window manager with off-screen buffering. Off-screen buffering means you can't directly draw into the screen, but your drawings go to the off-screen buffer*. From the off-screen buffer, it is combined with other drawings and form the final screen the user will usually see. (Android-App-Market.com, 2013)

Media framework: Media framework provides different media codecs, which allows the recording and playback of different media formats on Android.

SQLite: SQLite is the main database engine used in Android OS for data storage purposes

WebKit: This is the browser engine used to display HTML and related content

OpenGL: Used to handle 2D or 3D graphics content to the screen

Android Runtime:

Android Runtime consists of Dalvik Virtual machine and Core Java libraries.

Dalvik Virtual Machine:

It is a type of JVM (Java Virtual Machine) used in Android handheld devices to run apps and is optimized for low processing power and low memory environments. *Unlike the JVM, the Dalvik Virtual Machine doesn't run .class files, instead it runs*

.dex files. .dex files are built from .class file at the time of compilation and provides higher efficiency in low resource environments. *The Dalvik VM (virtual machine) allows multiple instance of Virtual machine to be created simultaneously, providing security, isolation, memory management and threading support. It is developed by Dan Bornstein of Google*. (Android-App-Market.com, 2013)

Core Java Libraries:

These are different from Java Standard Edition (Java SE) and Java Micro Edition libraries. *However these libraries provide most of the functionalities defined in the Java SE libraries*. (Android-App-Market.com, 2013)

Application Framework:

These are the blocks or programs that the applications directly interact with. These programs manage the basic functions of the mobile phone like resource management, voice call management and many others.

Important blocks of Application framework are:

Activity Manager: Manages the activity life cycle of applications
Content Providers: Manage the data sharing between applications
Telephony Manager: Manages all voice calls. We use telephony manager if we want to access voice calls in our application.
Location Manager: Location management, using GPS or cell tower
Resource Manager: Manage the various types of resources we use in our Application. (Android-App-Market.com, 2013)

Applications:

Applications are the top and last layer in the Android architecture and this is where the applications are fitted. *Generally, several standard and typical applications come pre-installed with every device, such as:*

SMS client app

Dialer

Web browser

Contact manager (Android-App-Market.com, 2013)

The outline above explains all the components of Android operating system architecture but it does not include the security features of Android OS in detail. For this reason the author will try to consider further examination of the Linux Kernel in terms of security features, as this is one important part of the thesis.

3.3 LINUX SECURITY MODEL FOR MOBILE PLATFORM

Linux security model is based on several strategies and concepts, including the CIA model. This stands for Confidentiality, Integrity and Accessibility. *Confidentiality is a CIA triad concept that relates to preventing the unauthorized disclosure of private information, such as usernames, passwords, and salary data.* (Jang, 2011)

Integrity is a CIA concept that means you can trust the data. It means only authorized users can change data.

Availability means users can have access to their data when they want it. The CIA concept of availability is important to users. (Jang, 2011)

This above mentioned model is applied to the Linux platform in general. But in this part of the thesis the author tried to look into the Linux security model for the mobile platform, which will still include parts of the CIA concepts.

Linux is the main part of the Android operating system and much of the Android security model is a result of that.

Most importantly to Linux security is the concept of users and groups. Each user in a Linux system is assigned a user ID (UID) when they are created. This is represented by a number and is used to differentiate one user from another.
Users can belong to specific groups and each group has a group ID (GID), which is just another number and it is used to differentiate one group from another. As a result, a user can be a member of multiple groups and consequently each group can have multiple members.
Permissions are assigned to each resource on a Linux system, with a resource typically being a file (almost everything in Linux is viewed as a file). Each resource has a defined owner, which is the UID of the user that has primary responsibility for the file and can alter the permissions on it.
Each resource also has a defined group, which is the GID of the group of users who have a set of permissions over and above that of the world, which is the group of all users on the system. (Six, 2012)

Each resource on a Linux system has three sets of permissions: owner, group, and world. So one file will have a set of permissions that apply to its owner, a set of permissions that apply to its group, and a set of permissions that apply to anyone that is not the owner or in the group that the resource is associated with (i.e. everyone else that has an account on the system).

Each set of permissions can include read (R), which allows that entity to read the file; write (W), which allows that entity to write/update the file; and execute (X), which allows that file to be executed as runnable code. It has to be noted that having read permission does not mean you have write permission, and also the opposite is true. *Linux permissions are also based on the idea that if you are not granted a certain right, you do not have it. So if a specific file has read and write access set for the owner and the group, but no permissions set for the world, if you are not the owner or in the file's group, you have no access to it*. (Six, 2012)

It is clear from the above Linux security model that access rights (read, write and execute), play a very important role in securing the system. These access rights work hand in hand with the three sets of permissions i.e. User ID (UID), Group ID (GID) and world.

3.4 ANDROID MASTER KEY VULNERABILITIES

The Master Key vulnerability is very recent and it was discovered by a security group called Bluebox. This security group is made up of well-known security developers who are dedicated in the fight against mobile platform attacks. Through a research, the security team discovered vulnerability within the Android security model that allows an attacker to turn any legitimate application into a malicious Trojan horse. The hacker tries this by modifying the APK (Application Package File) code without modifying the application's cryptographic signature. The Android Application Package file (APK) is the file format used by Google's Android operating system to distribute and install applications. An application package file contains many elements, including the app's code and certificates. Android apps generally come with digital signatures. A digital signature is what makes an application valid and true. Digital signatures confirm the identity of an app's developer and they ensure that future updates are issued solely by the app's developer. Breaking the cryptographic signature of any app is an indication that the app has been modified. The Maser Key vulnerability does not only allow the hacker to make these changes to Android apps, but also the changes made are unnoticed by the app store, mobile device, and end user. (About.com, 2014)

3.5 MOST COMMON DEFENCES

- Use of Android Antivirus app
- Identifying the app's publisher you want to install
- Downloading from Google Play Store

3.6 ANDROID OS VERSIONS

In order to distinguish clearly the different versions or updates of Android operating system over the years, the author tried to arrange the version according to their application programming interface (API) levels. The specifications for each update were not included by the author of the thesis.

Source: (WAFTR.COM | Tips - Tricks, 2014)

API Level	Version	Codename	Release date	Linux Kernel	Device/Features (e.g.)
1	Android 1.0	--------	23 Sep. 08		HTC Dream
2	Android 1.1	--------	09 Feb. 09		HTC Dream
3	Android 1.5	Cupcake	30 Apr. 09	2.6.27	HTC G1
4	Android 1.6	Donut	15 Sep. 09	2.6.29	Dell Mini 3
5	Android 2.0	Eclair	26 Oct. 09	2.6.29	Motorola Droid
6	Android 2.0.1	Eclair	03 Dec. 09	2.6.29	Samsung wave II
7	Android 2.1	Eclair	12 Jan 10	2.6.29	Samsung wave II
8	Android 2.2 – 2.2.3	Froyo	20 May 10	2.6.32	Dell Flash 3.5
9	Android 2.3 – 2.3.2	Gingerbread	06 Dec. 10	2.6.35	Google Nexus S
10	Android 2.3.3 – 2.3.7	Gingerbread	09 Feb. 11	2.6.35	Samsung Galaxy S, Nexus S 4G
11	Android 3.0	Honeycomb	22 Feb 11	2.6.36	Motorola Xoom
12	Android 3.1	Honeycomb	10 May 11	2.6.36	
13	Android 3.2	Honeycomb	15 July 11	2.6.36	Google TV enabled devices
14	Android 4.0 – 4.0.2	Ice Cream Sandwich	19 Oct. 11	3.0.1	Samsung Galaxy Nexus
15	Android 4.0.3 – 4.0.4	Ice Cream Sandwich	16 Dec, 11	3.0.1	Bug fixes and optimizations
16	Android 4.1	Jelly Bean	09 July 12	3.0.31	Nexus 7 Tablet
17	Android 4.2	Jelly Bean	13 Nov. 12	3.4.0	Nexus 4 & 10
18	Android 4.3	Jelly Bean	24 July 13	3.4.0	Nexus 7
19	Android 4.4	KitKat	31 Oct 13		Nexus 4

Source: Author, 2014

3.7 Market share Comparison of Android OS and Apple iOS

According to a study done by the International Data Corporation (IDC) worldwide Quarterly Mobile Phone Tracker, Android OS and apple iOS ranked top operating systems used in smartphones worldwide with 95.7% of all smartphones shipments during the fourth quarter of 2013. (IDC Analyze the Future, 2014)

3.7.1 Android OS

Android is well on the way to being the dominant power in smartphone's by reaching triple digits growth for the year 2013. Samsung played a very important role in Android success by getting 42.0% of smartphones shipments during the year. IDC reported: *Following Samsung was a long list of vendors with single digit market share, and an even longer list of vendors with market share less than one percent. The intra-Android competition has not stifled companies from keeping Android as the cornerstone of their respective smartphone strategies, but has upped the ante to innovate proprietary experiences.* (IDC Analyze the Future, 2014)

3.7.2 Apple iOS

Apple iOS maintained another quarter and a year of double-digit growth with a high demand for the iPhone smartphones. Perhaps the most is important feature is how iOS's year-over-year growth has begun to level out as compared to the overall market. Recent figures show that the iPhone market has fallen slightly as compared to a large growth of the Android OS.

4 Analytical part

4.1 Survey

A short survey was conducted from around Prague and online. The participants of the survey were people who use various Android smartphones. The main purpose of the survey was to investigate how each responded normally download apps, in particular downloads from Google market or downloads done anywhere on their smartphones just on the internet. The formulated questions were very basic and precise so as to avoid ambiguity.

Part of the survey was made by the author and put online to collect responses from close friends and relatives. The author was able to obtain around 55 participants who fully took part in the survey and the results were collected. The number of participants was not particularly high but it was still sufficient to conduct a study.

4.2 Hypothesis Testing:

1. **Chi-square test:**

The **null hypothesis** is that Android users are aware of malware risk in downloaded applications outside Google market

The **alternative hypothesis** is that Android users experienced malware downloaded in applications outside Google market more than in applications from Google market.

Below is the list of the questions that were part of the survey:

- Which version of Android smartphone to you use?
- How often do you download apps using your Android smartphone?
- Did you experience any malware through apps downloaded from Google market or outside Google market?

Data collected from the survey was put into IBM SPSS Statistics Software for analysis, the results are presented below:

IBM SPSS Statistics Results:

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Android user * Malware experience	**55**	**100.0%**	**0**	**0.0%**	**55**	**100.0%**

Source: Author, 2014

Android user * Malware experience Cross tabulation				
Count				
		Malware experience		Total
		yes	no	
Andr oid user	yes	**28**	**3**	**31**
	no	**14**	**10**	**24**
Total		**42**	**13**	**55**

Source: Author, 2014

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	**7.669**[a]	**1**	**.006**		
Continuity Correction[b]	**5.999**	**1**	**.014**		
Likelihood Ratio	**7.840**	**1**	**.005**		
Fisher's Exact Test				**.009**	**.007**
Linear-by-Linear Association	**7.530**	**1**	**.006**		
N of Valid Cases	**55**				
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 5.67.					
b. Computed only for a 2x2 table					

Source: Author, 2014

From the Pearson Chi-square: X^2 =7.669

Degree of freedom (df) = 1

(p value) is given by Asymp. Sig. = 0.006

This therefore means p < 0.05, the p value is less than the conventionally accepted significance level of α=0.05 and the null hypothesis is rejected. P < α

The same calculation can also be done as follows:

For a 2 x 2 contingency table, Chi square is given by the formula: $X^2 = (ad – bc)^2 (a+b+c+d) / ((a+c)(b+d)(a+b)(c+d))$, where:

Variable 2	Data type 1	Data type 2	Totals
Category 1	a	b	a + b
Category 2	c	d	c + d
Total	a + c	b + d	a + b + c + d = N

Source: (The Chi Square Statistic, 2014)

The Chi Square = $X^2 = ((238)^2 \times 55)) / ((42) \times (13) \times (31) \times (24)) = 7.669$

Interpretation: The alternative hypothesis is accepted and it states that Android users experienced malware downloaded in applications outside Google market more than in applications from Google market.

2. **<u>One sample t-test</u>**:

- The null hypothesis is that end-users have **never** had malware downloaded on their smartphones outside Google market.
- The alternative hypothesis is that users who download and install apps outside Google market had **at least once** downloaded malware.

In this part of the thesis the author tried to use **one sample t-test**, which relates the information from the respondents with a specific theoretical mean value. The author chose the mean value to be tested to equal 1, i.e. test value = 1.

Survey question:

I. How often do you end up downloading unwanted apps or catching viruses on your on mobile internet outside Google market?

- never
- once
- two times
- three times
- More than three times

The results from IBM SPSS Statistics Software:

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
Malware on mobile internet	55	1.4727	1.24506	.16788

Source: Author, 2014

One-Sample Test						
	Test Value = 1					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Malware on mobile internet	**2.816**	**54**	**.007**	**.47273**	**.1361**	**.8093**

Source: Author, 2014

p (*significance*) value = 0.007

$p < \alpha$

0.007 < 0.05 (we reject Ho hypothesis) »» The null hypothesis is rejected.

Interpretation: The results mean that we select the alternative hypothesis, which that the end-users had at least once downloaded malware outside the Google market.

4.3 Short introduction to MCA method

This method is used in decision making where there exists multiple and conflicting criteria. Such problems are a common occurrence in everyday life.

Basic concepts of MCDM:

Multiple objectives/attributes

- *Each problem has multiple objective/attributes. A decision-maker must generate relevant objective/attributes for each problem setting.* (kol, 2014)

Conflict among criteria

- *Multiple criteria usually conflict with each other (for example the quality and price of goods).* (kol, 2014)

Incommensurable units

- *Each objective/attribute has a different unit of measurement.* (kol, 2014)

Design/Selection

- *Solutions to these problems are either to design the best alternative or to select the best one among previously specified finite alternatives.* (kol, 2014)

In this part of the thesis, the author used the information given on the figure below to set the criteria to compare the three most used mobile operating systems, Android OS, iOS, and Windows phone.

	android	iOS	Windows Phone	Blackberry	symbian
User Friendly	****	****	****	**	*****
Customisation	*****	***	**	****	**
Stability	****	****	****	***	****
Layout	***	**	*****	***	**
SNS Optimisation	**	**	****	*****	*
Apps & app store/market	****	***	*	**	**
Firmware Upgrade/Updates	****	***	**	*	**
Special Services	**	**	*	*****	*
Lost phone tracking	***	***	*	*	*
Virus Free	***	*****	*****	*****	***
Total	34	31	29	31	23

Source: (GEEKS Inc., 2014)

The author used the above listed figure to set the weights for the multi criteria analysis. The values were taken from an online research and are therefore valid. The figure above also shows that considering the criteria used, Android OS is the best choice with a score of 34. If we consider the three most used operating systems, then Windows phone comes last after iOS.

4.4 Comparison of Android OS, iOS and Windows phone

	Security of personal data	Antivirus	Privacy management	Stability	**Results**
Android OS	5	3	5	4	4.3
iOS	4	5	2	4	3.7
Windows phone	3	5	2	4	3.4
Weight	0.3	0.3	0.3	0.1	1.0

Source: Author, 2014

The results of this calculation also show that Android OS is the best with a weighted score of 4.3, followed by iOS (3.7) and Windows phone (3.4).

5 DISCUSSION

In this part of the thesis a short analysis will be done to compare each end user's behavior on their Android smartphones. The author tried to investigate where most of the end users download their apps, in particular focusing on Google play store or anywhere else on mobile internet and try to find out which group of end users usually runs into trouble by downloading or catching an unwanted program or a bug (malware).

This part will also include a small preview of the Apple iOS operating system and it can be generally said that the Apple iOS appears to be more secured as compared to Android operating system. Users on the Apple iOS never or very rarely end up catching bugs on their smartphones.

From the results of the survey, two main points were identified by the author:

Users of the Android operating system who normally download or install apps from Google play store (formerly Google Market) seem to experience few if not zero problems with unwanted programs or malware. In this regard, it is maybe safe to say the Google play store is more secure and Google has done an incredible job in inventing and updating the store and making it open source for software developers to contribute to its improvement. One of the reasons why end users trust Google play store is that generally only apps with trusted and verified certificates can find a place on the store (Google market).

Secondly, end users who use the latest version of the Android operating system software such as Jelly Bean also seem to experience fewer security issues as compared to users who still own older software.

The main reason for this discovery might owe to the fact that the newest updates come with improved security and they directly deal with previous identified security holes in the older versions.

The author also discovered that users who download apps from trusted sites, where the identity of the software developer is made public, also seem to experience fewer security issues. This includes sites with the root *https*. The group of end users, who experienced most of the security issues, was those who normally just download or install any app without double checking the origin of such apps. This may bring to mind one of the most important security measures, which is social engineering. This is sometimes referred as the first line of defense, and it encourages users to be more aware and wise when using the internet.

6 CONCLUSION

The main goal was to identify the main security threats on Android OS and from the results of the analytical part of the thesis, it can boldly be said that Android operating system is relatively very secure due to its undelaying support of the Linux kernel. Malware issues rarely occur on Android OS since most end users install apps through Google market which is a relatively very secure platform. One other aspect that makes Android OS secure is the fact that it is open source software, and software developers can make updates and even try to invent more ways to improve its security. But we also learned that no operating system or even any computer is completely safe unless is it switched off or not connected to a network. In the case of Android OS, we found out through a survey and analysis of the results of the survey that some end users had experienced malware downloads on their android smartphones. Even-though those end users who had malware issues, confessed to have downloaded the infected apps outside Google market. It is clearly more advisable for users to download apps for their Android smartphones only on Google market, because of its robust security checks, though sometimes loop holes exists in the security model, it is very much safer.

For users of Apple iOS, the preferred destination for apps download is the app Store, for the same reasons as for Android OS. Comparisons done in this thesis between Android OS, iOS and Windows phone revealed that Android OS was a much better choice for an operating system when considering criteria such as stability, security of personal data, virus free and many others. Other survey on comparison are easily available in the latest literature and also show that Android is a much better choice compared with other two. The price and the fact that many manufactures have a chance to manipulate with Android OS hardware might be one of the contributing factors as to why Android OS is dominant. A lot of smartphone manufactures build their smartphones on Android OS architecture, but in the case of iOS only iPhones use this operating system.

7 BIBLIOGRAPHY

Android-App-Market.com. (2013). Retrieved January 2014, from Android-App-Market.com: http://www.android-app-market.com/android-architecture.html

About.com. (2014, February 26). Retrieved 2014, from About.com Computing>Antivirus Softwre: http://antivirus.about.com/od/virusdescriptions/a/Android-Master-Key-Vulnerabilities.htm

GEEKS Inc. (2014, March). Retrieved March 10, 2104, from geeks incorporated: http://geeksincorporated.wordpress.com/2012/06/09/which-is-the-best-smartphone-os/

IDC Analyze the Future. (2014, February). Retrieved Febraury 2014, from International Data Corporation : http://www.idc.com/getdoc.jsp?containerId=prUS24676414

The App Entrepreneur-The next Android version. (2014, February). Retrieved from The App Entrepreneur: http://theappentrepreneur.com/the-next-android-version-what-to-expect-for-developers

The Chi Square Statistic. (2014, March). Retrieved from HWS Math and CS: http://math.hws.edu/javamath/ryan/ChiSquare.html

WAFTR.COM | Tips - Tricks. (2014, March 10). Retrieved 2014, from WAFTR.COM | Tips - Tricks: http://2.bp.blogspot.com/-MS6X3WrdlKc/Uos1DFbh_HI/AAAAAAAAI2E/EC6W1uLxhIs/s320/Android_logic.png

Burnette, E. (2014, March 2). *ZDNET*. Retrieved February 12, 2014, from zdnet.com: http://www.zdnet.com/blog/burnette/how-android-works-the-big-picture/515

Hoog, A. (2011). *Android Forensics.*

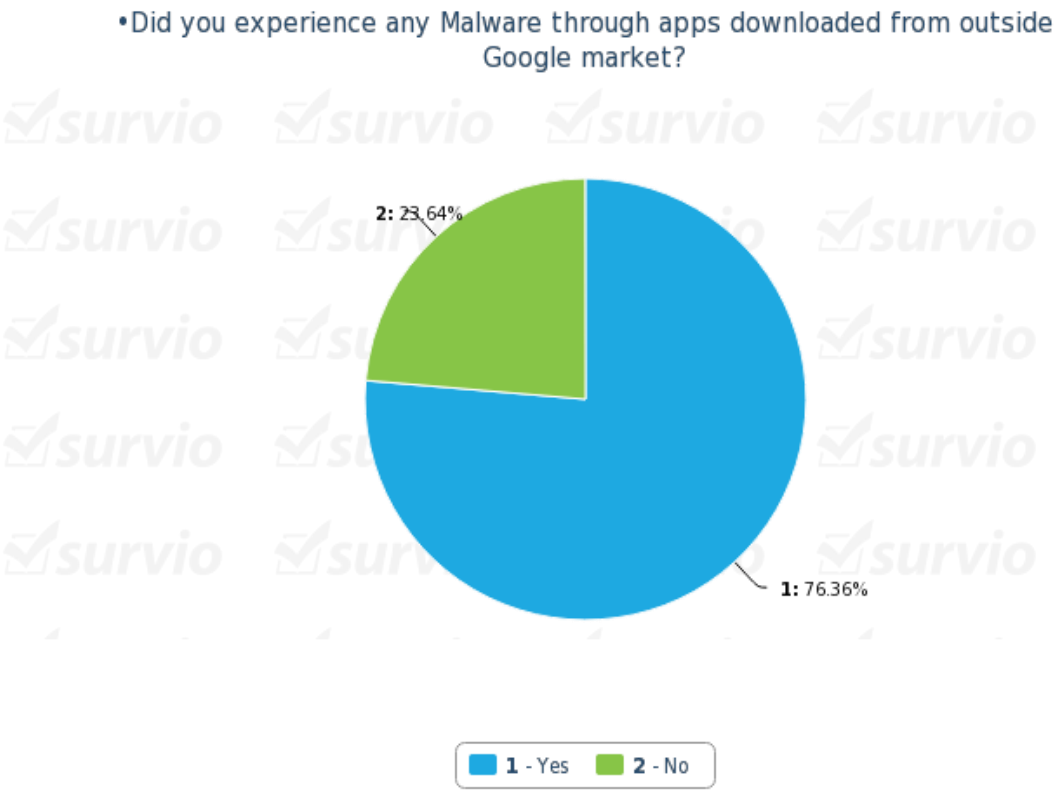
Jang, M. (2011). *Security Strategies in Linux Platfrom and Application.* Jones&Bartlett Learning, LLC.

kol, Š. T. (2014). *Distance Learning Module for Management Science.* Retrieved March 2, 2014, from Multiple Criteria Decision Making: http://orms.pef.czu.cz/text/Multicriteria/MCfirstLevel.html

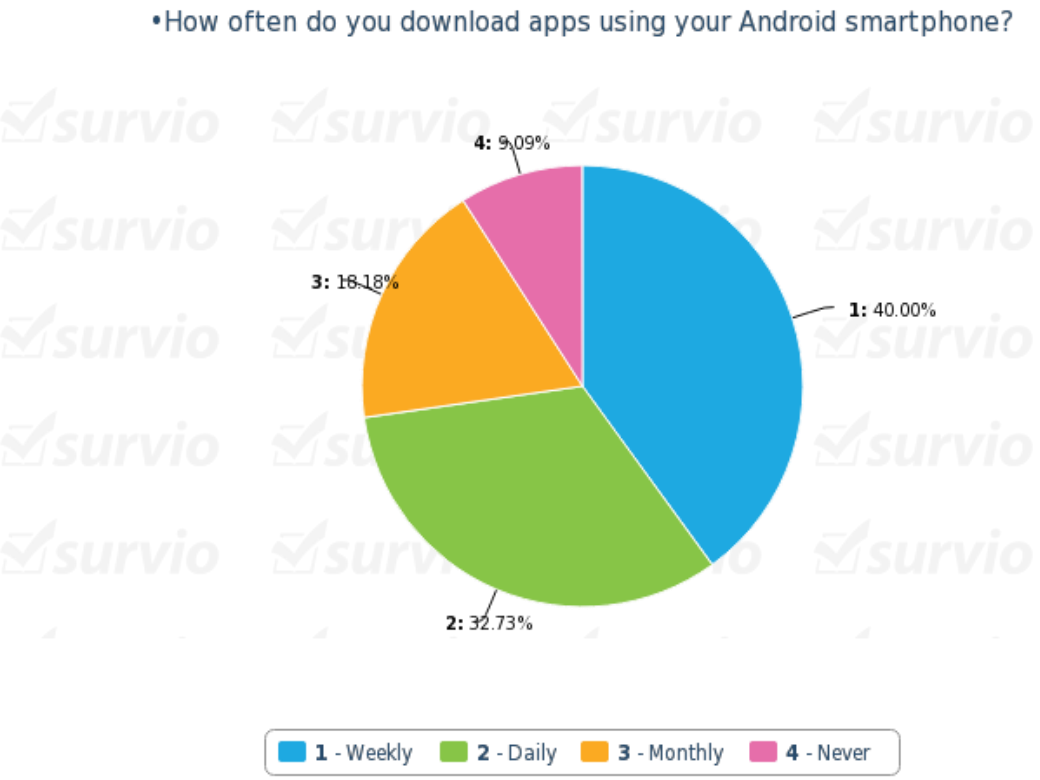
Six, J. (2012). Application Security for the Android Platform. In J. Six, *Application Security for the Android Platform.* CA: O'Reilly Media Inc.

8 SUPPLEMENTS

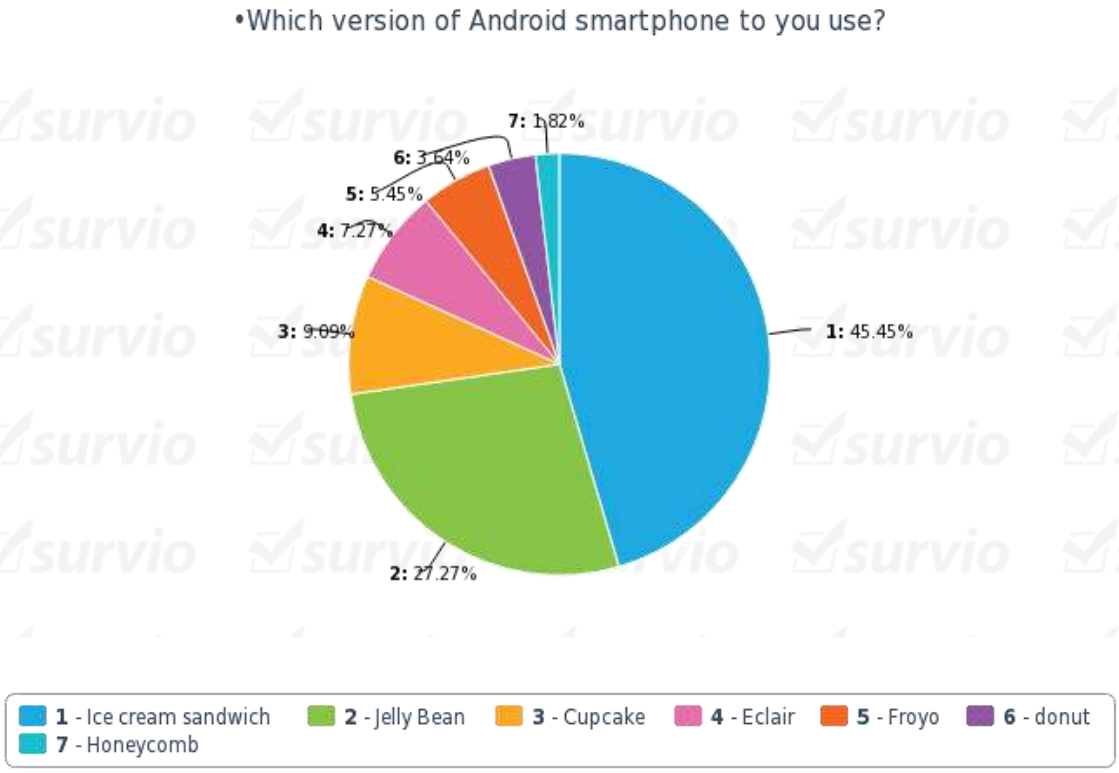
Below are the questions and results of the survey that was carried out during the writing of this thesis:



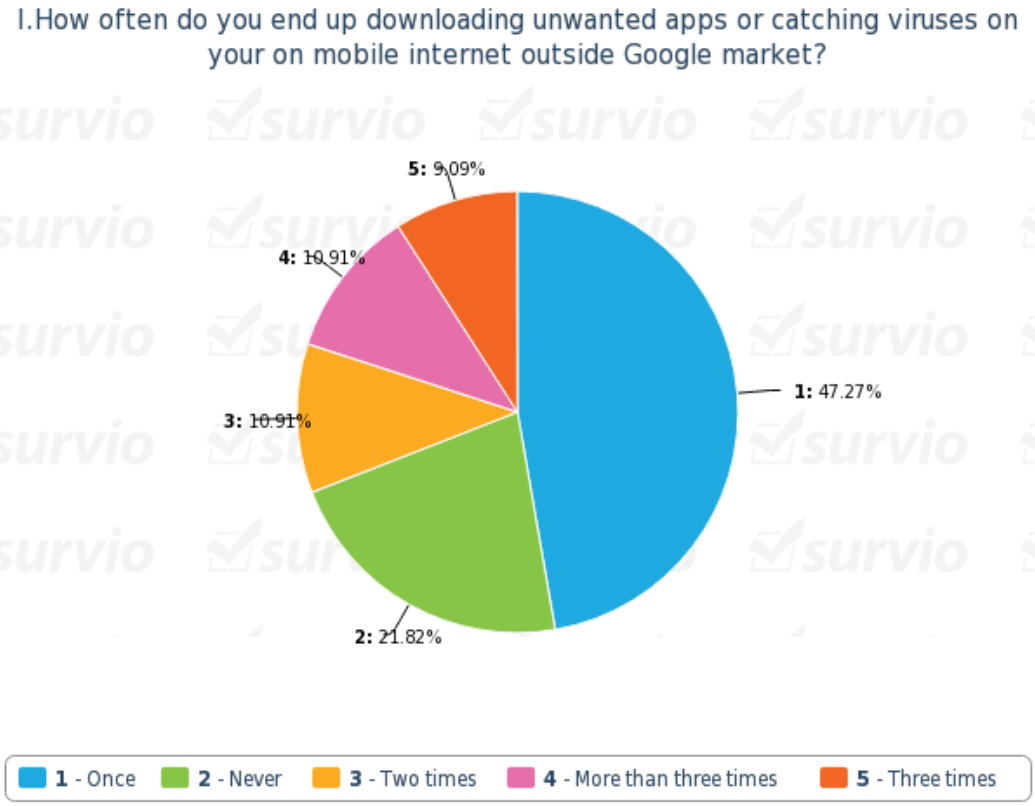
Source: Author, 2014



Source: Author, 2014



Source: Author, 2014



Source: Author, 2014