ALMA MATER STUDIORUM · UNIVERSITA' DI BOLOGNA

Campus di Cesena - Scuola di Scienze

Corso di Laurea in Scienze e Tecnologie Informatiche

The Secret Life of Software Applications

Relazione finale in
Reti di Calcolatori

Relatore
GABRIELE D' ANGELO

Presentata da
PAOLO DELL' AGUZZO

II Sessione
Anno Accademico 2013 - 2014

"Society exists only as a mental concept.
In the real world there are only individuals."

- Oscar Wilde

Abstract

One of the most undervalued problems by smartphone users is the security of data on their mobile devices. Today smartphones and tablets are used to send messages and photos and especially to stay connected with social networks, forums and other platforms. These devices contain a lot of private information like passwords, phone numbers, private photos, emails, etc. and an attacker may choose to steal or destroy this information.

The main topic of this thesis is the security of the applications present on the most popular stores (App Store for iOS and Play Store for Android) and of their mechanisms for the management of security.

The analysis is focused on how the architecture of the two systems protects users from threats and highlights the real presence of malware and spyware in their respective application stores. The work described in subsequent chapters explains the study of the behavior of 50 Android applications and 50 iOS applications performed using network analysis software. Furthermore, this thesis presents some statistics about malware and spyware present on the respective stores and the permissions they require. At the end the reader will be able to understand how to recognize malicious applications and which of the two systems is more

suitable for him. This is how this thesis is structured. The first chapter introduces the security mechanisms of the Android and iOS platform architectures and the security mechanisms of their respective application stores. The Second chapter explains the work done, what, why and how we have chosen the tools needed to complete our analysis. The third chapter discusses about the execution of tests, the protocol followed and the approach to assess the “level of danger” of each application that has been checked. The fourth chapter explains the results of the tests and introduces some statistics on the presence of malicious applications on Play Store and App Store. The fifth chapter is devoted to the study of the users, what they think about and how they might avoid malicious applications. The sixth chapter seeks to establish, following our methodology, what application store is safer. In the end, the seventh chapter concludes the thesis.

Prefazione[1]

L'utilizzo di smartphone e tablet sta diventando sempre più frequente tra persone di qualsiasi sesso ed età. Un problema preso poco in considerazione è quello della sicurezza dei dati contenuti all'interno dei dispositivi mobili. Sempre più utenti utilizzano i loro dispositivi per inviare messaggi, scattare foto, inviare e ricevere mail, comprare online, passare del tempo sui social network, ecc. senza essere consapevoli dei pericoli a cui vanno incontro.

In questa tesi viene descritto in quale modo Google ed Apple controllano i rispettivi negozi di applicazioni e in quale modo le architetture dei sistemi Android e iOS sono in grado di difendere l'utente da eventuali minacce. Dunque viene illustrato in quale modo, tramite software di analisi di rete, è stato possibile individuare applicazioni malevoli. Infine il lettore sarà capace di riconoscere le applicazioni malevole e di capire quale tra i due sistemi, iOS ed Android, sia più adatto al suo utilizzo.

La tesi è così strutturata. Il primo capitolo introduce i meccanismi di sicurezza adottati tramite l'architettura delle due piattaforme e dunque quelli relativi al controllo delle applicazioni nei rispettivi store.

---

[1] This section was added to fulfil "Università di Bologna" 's requirements for non-Italian thesis. The rest of the thesis is written in English.

Infine spiega quale tipo di applicazioni malevoli ci interessa particolarmente. Il secondo capitolo spiega come è strutturato il lavoro, quali sono gli strumenti utilizzati e perché. Il terzo capitolo introduce il protocollo seguito per i test, l'esecuzione reale dei test e la modalità con la quale abbiamo definito il reale livello di pericolo di ciascuna applicazione. Il quarto capitolo mostra i risultati ottenuti e illustra alcune statistiche relative alla presenza di applicazioni malevoli nel Play Store e nell'App Store. Il quinto capitolo è incentrato sul pensiero degli utenti nei riguardi della sicurezza Android e iOS e propone delle linee guida da rispettare per evitare di installare malware sul proprio dispositivo. Il sesto capitolo ha lo scopo di far riflettere il lettore su quale tra Android e iOS è attualmente la piattaforma più sicura e adatta a lui. Infine, nel settimo capitolo, si conclude la tesi.

Table of Contents

List of Figures

Chapter 1

Introduction to Mobile Security

This chapter has the aim to explain how is security handled in mobile devices focusing on those who have iOS or Android systems. First, we observe security management in the two systems and after we give an explanation on how Google and Apple work to ensure security to users who download applications (apps) from their respective stores.

1.1 Android Platform

Android is developed by Google. It is a Linux based operating system and uses the Linux Kernel [1, 21].

The main levels of the Android platform architecture are (from lower to higher) [1]:

1. Linux Kernel;
2. libraries/Android runtime;

3. application framework;
4. application.

1.1.1 Security Aspects of the Android Platform

The four levels listed ensure isolation between processes and especially the sandboxing mechanism [1, 2].

The sandboxing mechanism works this way. Every time an application is installed on device, it receives a unique User ID (UID) and a group ID. This guarantees that two different applications cannot run in the same process. If two or more apps need to share the same process or the same permissions set, they must request a specific UID called Shared User ID even if this is possible only when these applications are signed using the same signature.

Using this mechanism it is possible to avoid that an application starts compromising data that are owned by the system or another application. Furthermore, in this way, an application that does not have the right permissions cannot access to Global Positioning System (GPS), Camera, Network Communication, etc. and all those tools for which permissions are required.

1.1.2 Permissions Required by Applications

Each application may require some permissions. Apply for permissions is the only way for an application to access some features of the smartphone that otherwise would not be accessible (like GPS and camera). Programmers are obliged to declare the permissions necessary for the application they developed and therefore to include them into a file called AndroidManifest.xml[2] [10].

If a programmer does not declare permissions, the application cannot run in the device in which it is installed [3]. However, permissions play a big role even for the users because when someone wants to download an app from Google Play, he (or her) could read all the permissions declared in the manifest file of the application. It's very important to read them because, as we shall see, users can recognize malware and spyware also by means of permissions.

1.1.3 Memory Randomization

The process that we are going to describe now is called memory randomization or address space layout randomization (ASLR) [4] and it's a process with the purpose of allocating memory, shared libraries, data

[2] The Manifest file is bundled into the Android installation package file. It provides all the necessary information to the Android platform for the execution of the application [10].

and others of an application randomly. Through this process, Android system ensures that a malware cannot attack the memory of a running app.

However, a programmer must be careful because it's his responsibility to prevent buffer overflows and memory corruptions [4].

1.2 iOS Platform

iOS is developed by Apple and it is derived from OS X, the operating system (OS) of MacBook and iMac. iOS is an operating system available only for iPhone and iPad made by Apple Inc. contrary to Android that develops an OS for a greater range of smartphones and tablets.

The four principal layers of iOS platform architecture are (from lower to higher) [4]:

1. Core Os Layer;
2. Core Services Layer;
3. Media Layer;
4. Cocoa touch layer.

1.2.1 Security Aspects of the iOS Platform

The sandboxing mechanism is also present in iOS systems and has been defined by Apple as a set of fine-grained control that limits the app

access to file system, network and hardware [4]. Even memory randomization is also present in iOS and it has the same behaviour seen for Android. However, Apple does not release much information about mechanism of its security system and is not the main purpose of this thesis to dwell more on the architecture and security of the system.

1.3 Security on Application Stores

The main target of this thesis is not to understand how is made or how work the architecture of the two different systems. We know now that the two systems, Android and iOS, have four layers that work together not just with the aim of running applications, but even with the purpose of guaranteeing security for applications, user's data and even for the system in its entirety.

The main purpose of this work is to understand if Apple and Android teams do something to prevent users from downloading malicious applications and to stop developers who want to publish malicious applications.

The official application stores are really full of malware and spyware. In 2013 Google Play Store had more than 42000 known malicious applications [12].

1.3.1 Google Play Store

Google Play Store is the official application store made by Google for Android devices. Each user can choose to take a look using the application on device or the website. In this store we can find one search bar and some buttons for the categories like Applications, Music, Films. When someone searches a game, for example, he (or her) can choose to search it using the search bar or the appropriate category.

Users can download a lot of applications in this store, precisely in 2013 the number of apps already exceeded 1 million and every day many applications are uploaded [5].

Once user has found the app of interest, the store presents a page with the app's logo, some screenshots or photos, a description and ratings and reviews submitted by other users. Choosing to download the application, the Play Store puts in front of the user a list of permissions that the app required for its execution. At this point user can choose to accept the condition and install the application, allowing all the permissions required, or to deny it.

1.3.2 Google Play Store Security

The security of the Play Store is determined by visible and invisible elements. Play Store shows us the permissions required by the app we want to download and this is a form of security, visible, which requires the

diligence of the user to avoid downloading malicious application. The invisible element is called *Bouncer*. Google announced this security mechanism only recently and its malware detection techniques are not available publicly. However, this tool scans all the applications loaded on Play Store soon as they are loaded and before they are available to the public. Bouncer dynamically and statically analyses the binaries of the applications that are submitted to be included in the Play Store [6, 7].

1.3.3 iOS App Store

iOS App Store is the official application store made by Apple for iOS devices. Users can choose to search an app using the search bar or browsing between categories like Game, Child, Food and Drinks.

Users can download a lot of apps from the App Store. In 2014 the store made by Apple exceeded 1 million applications (precisely App Store has fewer applications than Google Play Store) [8]. When a user chooses the app he wants to download, the App Store puts in front of him some details composed by description of the app, information about author, application's logo, screenshots, the developer's website, and it shows the reviews and ratings. In contrast to the Play Store, permissions are not shown because there is no security mechanism based on permissions in iOS devices [22].

1.3.4 iOS App Store Security

The applications available into the App Store are checked by a review process, but information about how apps are checked is not available to the public [6]. Probably, every time a developer wants to publish an app, someone checks if the application contains illegal, adult and other unfair contents. Precisely Apple announced: «We will reject Apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.» [9].

It is not known how Apple discovers malware, however it's very important to point out that when Apple or other users discover a malware or a spyware within the App Store, this is removed remotely from all the devices that have it installed and from the store [10].

1.3.5 Other Application Stores

Unfortunately users can download applications even from unofficial stores. This is not true if you are an iOS user unless you jailbreak[3] your iPhone or iPad. If you are an Android user, there is the possibility to download apps from unofficial applications stores and this is unsafe for

[3] Jailbreaking is the name given to the process used to modify the iOS operating system to allow user greater control over the device including the ability to install apps from unofficial stores.

data present on device. While Google Play Store and iOS App Store declare that there are some security mechanisms, the unofficial markets have no security mechanism declared and often they contain all the applications that Google or Apple teams have refused from their store.

1.4 Application Based Threats

During the next chapters we describe how we have searched and found malicious applications, but we have to define now what kind of malicious app we targeted.

There are four main types of application based threats [1]:

- **Spyware**: applications that collect user's information without user's consent.
- **Malware**: applications that destroy data on device, attempt to block the device, send messages without user's consent and do other actions that may undermine the stability of the device.
- **Privacy Threats**: applications that want access to data not really necessary to execute their tasks.
- **Vulnerable Applications**: applications with some vulnerabilities that an attacker can use for remote control of the device, to have some specific permissions or to download a malware without user's consent.

What we are going to show is the behaviour of some applications observing for first the network activity. All the apps that steal data and undermine the privacy (for example apps that steal emails, address book contacts, chronology, bookmarks, etc.) are spyware and privacy threats. As already said for Android system is always necessary to declare permissions, so technically a user, when downloads an application, gives always his consent. Privacy threats and spyware will be for us the same thing.

In addiction to network activity, we will observe even some surface behaviours like the activation of GPS for no reason, the continuous activation of some processes as soon as we close them and the continuing advertising sent to screen with no application visible on screen. The applications with these behaviours are malware, however in this work we have not analysed the code of each application and we do not have found apps that can compromise the stability of the device. The applications selected have been chosen randomly with the aim to search especially privacy threats and little weight malware. Malware with the aim of making the device unusable using or not vulnerable applications were not found and are not of our interest[4].

[4] We considered only malware with a visible bad behaviour. As we shall see, tests are made on virtual machine, so we do not know if some tested applications are capable of compromising a real device.

1.5 Summary

In this chapter we have seen how Android and iOS platform architectures work to ensure security. Both have a sandboxing mechanism and a memory randomization mechanism. In this way the two systems ensure that no application can do any dangerous action without permissions and that no application can damage data of another app.

After that, we have seen how are made the Google Play Store and iOS App Store recognising that both have security mechanisms. These security mechanisms serve both to assess the content visible to the users and to evaluate the content harmful for the device that may be invisible for the users. Google and Apple do not give more information about these mechanisms, probably because, if an attacker understands how they work, they become easier to get around [6, 11].

At the end we have defined four types of threat deriving from malicious applications and we explained that we will discuss especially about privacy threats and spyware and less about malware.

Chapter 2

Setup of the Test Environment

This chapter describes the tools used for the network analysis and why we have chosen them. Regarding Android, we begin with the description of the OS used and the description of its firewall. After that, we focus on the virtual machines and we describe the network analysis software and the tests done. Regarding iOS, we introduce another methodology and especially we will no longer need virtual machines.

2.1 Setup of the Android Test Environment

Our choice on how to analyze the behaviour of the Android applications has been to use a personal computer (PC), with Windows 7 Home Premium OS, running the network analysis software and the virtual machine (vm).

2.1.1 Windows Firewall

The reason why we need to configure the firewall is that our goal is to analyze the network to see all the packets sent and received by the vm chosen. So, we want to configure the firewall to block all the packets sent and received by other software installed on the host.

A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings [13].

Windows firewall is managed at operating system level and allows the management of different profiles (home network, corporate, private or other user-defined) which each has set different rules. These rules can define different settings with regard to incoming and outgoing connections. They can be related to an Internet Protocol Address[5] (IP) or to a specific port.

To configure the firewall we decided to use PC Tools Firewall Plus 7 [14], a software that allows us to observe in real time what program requires access to the network. By this software we can block the incoming ports and/or the outgoing ports of each program. Consequently, we use PC Tools Firewall Plus 7 to block the connection of all the programs except for the virtual machine.

[5] An IP is a numerical label assigned to each device participating in a computer network that uses Internet Protocol for communication.

2.1.2 Network Analysis Software

Once we have configured the firewall we need a network analysis software with the aim to capture the packets exchanged in our network[6]. Through this software, we will be able to observe the network packets of the apps running on the virtual machine and, at the same time, we will use it to determine which virtual machine is active on the network only when we do something (like surfing the net, running an application, etc.).

The software we need is called Wireshark and it's a network packet analyzer that tries to capture network packets and tries to display that packet data as detailed as possible [15].

2.1.3 Virtual Machines

To conduct this analysis, it was necessary to decide which of the available virtual machines use. Surfing the net it's possible to find different types of virtual machines made to play, or to emulate a device or to develop applications. The virtual machine that we are searching must observe the following requirements:

---

[6] A device, connected to a network, exchanges information with other devices connected. This information is collected in a packet that consists of two kinds of data: control information and user data (or payload). The control information provides data the network needs to deliver the user data, like source and destination network address.

- it has to work smoothly;
- must have the Google applications (GApps);
- must give us the opportunity to have superuser rights within the emulated device;
- must give us the possibility to drag and drop.

After a period of research, we have finally identified the best environment. The virtual machine selected is Oracle VirtualBox [16] with the plugin Genymotion 2.1 [17]. The Oracle VirtualBox is a very fast vm and Genymotion is a very rapid emulator for Android. These two tools help us satisfy the requirements seen above.

At this point, we have created an Android emulated device with Android 4.1.1, that is Application Programming Interface 16 (API). Thanks to the drag and drop function we could send files[7] with the purpose to acquire superuser rights and to have Google applications[8].

[7] Surfing the net, the reader can find all the archives mentioned in this thesis, but we can't link them.

[8] GApps are all the applications made by Google. We are particularly interested in the Google Play Store. Google doesn't release its apps because more and more people are using virtual machines to emulate Android devices.

2.1.4 ARM Architecture and x86 Architecture

Testing our emulated device, we realised that there was another problem. Some applications are developed only for Advanced RISC Machine (ARM) architecture, which is used especially on mobile devices like smartphones and tablets.

ARM Architecture indicates a family of 32-bit RISC microprocessors that provides excellent performance and a low battery consumption, which is why it is used on almost all smartphones and tablets [18].

x86 Architecture indicates a family of CISC microprocessors and the instructions are of variable length. In contrast to the ARM architecture, this is used mostly in the PC Desktop [18].

To get around this problem it's possible to find, surfing the net, three archives that help us perform the translation from ARM architecture to x86 architecture (the three archives are called *ARM_LIB*, *libhoudini* and *libdvm_houdini*).

2.1.5 Network Activity of the Virtual Machine

The last phase of the research of the virtual machines focuses on the network activity of the virtual machine that before we have defined as the best. Our purpose is to find a vm that doesn't have network activity except when we induce it. In this way we can analyze only the activity of

the applications installed on the emulated device and not the activity of the vm presents for other purposes[9].

We have configured the firewall so that only the packets sent and received by the vm are present in the network. After that, we have done three tests to understand what virtual machine has the appropriate network activity:

1. The first test is to use the emulated device to scroll through the menu and to start some basic applications that don't require Internet connection. These apps are those found on a real smartphone as soon as a user buys it (like camera, calculator, alarm, calendar, etc.). By this test we are able to understand if the vm sends and receives packets for his purposes.

2. The second test is to use the browser and the Google search bar to search something on the web. Through this test we are able to recognize the packets captured by Wireshark sent and received for our guilt and those created for the vm purposes.

[9] For example, BlueStacks [19] presents network activity for other purposes because, every time a user moves through the menu, the virtual machine downloads the icons of all the apps in that screen from their reference sites.

3. The third test is to start and play some applications downloaded from Google Play Store. Through this test we have understood how the real network activity, that we will face on network analysis step, occurs.

Oracle VirtualBox has proven to be, even this time, the best vm tested. All these three tests have given us a positive response. Oracle VirtualBox with Genymotion is officially the virtual machine that we will use for the network analysis which will be discussed.

Regarding Android, we have a PC with the right firewall configuration now, a network analysis software and a virtual machine with superuser rights and Google Play Store. We can already start the network analysis phase.

2.2 Setup of the iOS Test Environment

Regarding iOS, we have chosen a different way to tackle the analysis phase. First of all we have chosen a Macintosh (Mac) with OS X Mavericks and we will not use a virtual machine.

With the availability of an iPad Mini with iOS 7 the choice has been to share the connection between the MacBook and the iPad. In this way the iPad turns out to be connected by the Mac connection and all the packets sent and received by the iPad have to pass through the network

card of the MacBook. So, using Wireshark installed on Mac to analyze the network, we can see the network activity of the iPad.

2.2.1 OS X Firewall

OS X is based on a Unix-like kernel, accordingly we have thought to start some captures to discover if we need a firewall or not. As we know, operating systems like those of Linux family (that are based on a Unix-like kernel) don't do anything suspicious or hidden from the user [20]. In addition, being a new MacBook, there were installed only the basic applications and Wireshark.

We have done many captures using the MacBook, scrolling through the menu, taking some pictures, etc. and there was no network activity. However, if we need it, there is already a firewall tool that you can configure in the OS X systems.

2.2.2 iPad Connection

As opposed to vm, we don't have to do tests to study the network activity of the iPad because fortunately we have a real device. So is sufficient to share the connection of the MacBook via Bluetooth and connect the iPad via Bluetooth with the Mac.

Being a new iPad, when we have done some tests to discover the behaviour of the device, we have seen that there was no network activity until we were to provoke it[10].

2.3 Summary

In this chapter we have described how to set up the test environment for Android and for iOS.

Regarding Android, we have decided that the best way to execute the tests is to use a PC with Windows 7 operating system. In this PC we will set the firewall appropriately through PC Tools Firewall Plus and we will use Wireshark for the packet capture. The analysis tests will be done using a virtual machine that emulates a device with Android 4.1.1. We have granted superuser rights to our emulated device and we have put into the device the GApps and the necessary libraries to translate from ARM architecture to x86 architecture.

Regarding iOS, we have decided to use a MacBook with OS X operating system. There is no necessity to set the firewall and we have installed Wireshark to capture network traffic. The analysis tests will be done using a real device, precisely an iPad with iOS 7. The PC will share its connection via Bluetooth and the iPad will exploit it.

---

[10] Having a new MacBook and a new iPad increases the probability that the two devices are not compromised.

Chapter 3

The Network Analysis

The network analysis is the main phase of our work. This chapter describes all the rules followed to conduct the analysis. It will define a protocol to follow and some “danger levels” related to the applications. The reader will know what kinds of apps have been analyzed and will be introduced to particular steps done only for Android or only for iOS.

3.1 The Protocol

The analysis that we will conduct needs some rules to follow. The protocol that we are going to define has to be efficient, functional and identical for all the applications that we are going to analyze. Following the protocol we are sure that we will do the same work for all the applications.

The protocol consists of these points:

1. open Oracle VirtualBox and after Genymotion;
2. start the vm with Android 4.1.1;
3. open Wireshark and start a new capture with promiscuous mode disabled;
4. stop the capture;
5. open PC Tools Firewall Plus and start the firewall to allow connection only for the virtual machine;
6. start a capture with Wireshark to ensure that the firewall is started;
7. stop the capture;
8. download the app you want to analyze from the Play Store \ App Store;
9. when the download is finished: close all the applications opened except for basic apps and basic processes;
10. start a new capture with Wireshark;
11. start the app downloaded and use it like a common user;
12. stop the capture;
13. observe if one or more new processes are started;
14. analyze the capture file.

Regarding iOS, we have to follow the same steps, but we can start from the eighth point. As we have seen above, we don't need a firewall configured and we don't use a virtual machine. So is sufficient to open the iPad, download the app we need and close other applications. After that, it is necessary to connect the iPad via Bluetooth with the PC that has shared its connection. At the end we can start a new capture with Wireshark and play the application downloaded like a common user.

3.1.1 Promiscuous Mode Disabled

During the capture it's better to avoid the promiscuous mode so that there are less irrelevant packets to analyze.

The promiscuous mode allows the user with superuser privileges to observe the packets sent and received by other computers connected in the same network. This is possible because some of these packets pass even through the network card of our PC.

3.1.2 Download from Play Store or App Store

First of all, we will download applications from Play Store, when we are going to analyze the Android environment, and from the App Store, when we are going to analyze the iOS environment.

Regarding iOS, we cannot see the permissions required by the applications because there is no security mechanism based on permissions.

However we have taken a screenshot of the download page of each application and we have saved it into a folder with the name of the application downloaded.

Regarding Android, we have taken the same screenshots especially with the aim to save all the permissions required by each application downloaded. This is very useful for the statistics on the permissions required by all the applications that we will describe.

Either way, we have created a folder for each application downloaded. Each folder has the name of an application and contains some screenshots, some capture files and even some notes when necessary.

3.1.3 Basic Applications and Processes

The main idea is that an application could use basic processes and basic applications to read, write and steal data. So, we don't want to close these basic applications and processes because we want to discover if the applications downloaded want to exploit them.

At the same time we want to close all the applications and processes opened that are not present in a new device. This because two or more malicious applications may want to access the same resource interfering with the application that we are analyzing.

At the thirteenth point, we have to check if new processes and applications are started. This verification is necessary to understand if

the app tested has open some basic processes previously closed or if the test is not valid because another application has interfered with the test.

3.2 Danger Levels

Danger levels are necessary to understand how much an application is dangerous for a user and his device. After the study of the capture file of each application, we determine what is the danger level of the application. Each application that appears to be dangerous for the users, has one or more notes with some screenshots that report the main malicious behaviour that we have discovered.

Later we will illustrate some statistics on malicious applications and on the stores of origin. So, we have decided to represent the danger levels with exclamation points in this way:

- **No exclamation points**: an application that doesn't seem to be malicious after two or more captures;

- **(!)**: an application that steals the International Mobile Station Equipment Identity (IMEI)[11] or the phone number without a known reason;

[11] IMEI is a unique code used to identify a device. Through the IMEI it's possible to block the use of a device. It's sufficient to insert the IMEI of a device in a black list of a provider to block it. The advice is to give the IMEI to no one [23].

- **(!!)**: an app that steals IMEI, phone number and other sensible data contained in the Subscriber Identity Module (SIM) Card and even in the Google / iTunes account registered on the device;

- **(!!!)**: an application that, in addition to what we have seen above, wants to steal data of other applications like the browser and enters into the address book and into the email accounts present on the device;

- **(!!!!)**: an application that tries to steal money and to enter in bank accounts. Furthermore, this application tries to send the content of some SMS, mails and MMS to its servers and to download files and other apps from unofficial stores or websites;

- **(!!!!!)**: an application that takes some pictures, records videos and sounds, sends SMS, MMS and mails without the user's knowledge;

All these actions mentioned must be understood as actions carry out without the user's knowledge.

Anyhow, after that we have decided what level of danger assign to an application, we have put before the name of its folder a number of exclamation points that reflects this level.

3.3 Choosing Applications

We want to choose the applications to test like a common user would choose them. So, we have decided to download applications with a high number of downloads and at the same time apps with a low number of downloads. We have taken well-known apps and not popular apps. We have chosen applications from all the continents and we have decided to download applications known to be safe and those known to be really unsafe.

Particular attention has been devoted to all those applications that required strong permissions like the use of camera, the possibility to read the call log, the possibility to send or read SMS, MMS and mails, etc. especially when it doesn't seem that the application observed needs really these permissions. At the end we will try to understand which permissions, if required together, may be indicative of a malicious application.

Regarding iOS, it's not possible to pay attention to permissions, so we have chosen the applications in a more random way. However, we have followed the same methodology described above. Obviously, the applications tested are not and they cannot be the same tested for Android. In this way, we cannot do an accurate comparison between the two architectures, but we will try to give an estimate of the security of the respective stores and their applications.

3.4 Summary

This chapter describes how to deal with the analysis of the applications. It has been defined a protocol to follow with the aim to test all the apps in the same way. After that, the reader has understood how each application will be marked to indicate how much is unsafe for the user and his device. This convention will be useful especially when we will want to discuss about some applications with the same level of danger. At the end, this chapter explains how we will choose the applications. We remind the reader that our purpose is to select randomly each app observing, during Android tests, the permissions required.

Chapter 4

Tests and Statistics

This chapter describes the results of the tests done on Android applications and on iOS applications. The reader will know how malicious applications work and when we have assigned a level of danger instead of another. After that, we will discuss about some statistics. The statistics are focused on the number of malicious applications and the ratio between the levels of danger. Regarding Android, this chapter explains how permissions work. Furthermore, we will discuss about what permissions required together could be unsafe for the user and / or the device.

4.1 Android Analysis

First we will discuss about the Android analysis phase. We have to create code names for each application because we don't have the opportunity to mention the real name. After that, we begin to see some statistics on Android environment.

4.1.1 Code Names of the Applications

The code name that we assign to each app is an alphanumeric code name with 4 characters. The first character it's a letter and follows this legend:

- **D**: app with the aim to download video and / or music;
- **G**: game;
- **L**: launcher or lock application;
- **M**: application for messaging and / or chat;
- **S**: social network application;
- **U**: utility application;
- **V**: application for viewing videos;
- **A**: app of another genre;

The remaining three characters are sequence numbers like 001, 002, etc. It's possible to find the same sequence of numbers, but only when the first character is different (for example D001, M001).

Now that we have decided the way to call the applications tested, we observe for each app the code name assigned and a brief description:

- **D001**: this app gives us the opportunity to download all the videos present on YouTube and other platforms. It's like a normal browser with a special button to download videos. It has been downloaded 10 million times and it has 244,130 ratings and reviews with an average rating of 4 stars;

- **S001**: this app presents to us like a social network and gives us the opportunity to interact with other users. It seems to be a compromise between Facebook, LinkedIn and a dating site. It has been downloaded 10,000 times and it has 300 ratings and reviews with an average rating of 4.3 stars;

- **L001**: this app allows you to unlock the smartphone using fingerprints like for the iPhone 5S. Obviously it's a funny joke to show to friends. It has been downloaded 10,000 times and it has 207 ratings and reviews with an average rating of 3.9 stars;

- **G001**: it's a soccer game in which you must slide your finger on the screen with the right speed and trajectory to simulate passing, shooting and perfect actions. It has been downloaded 5 million times and it has 412,111 ratings and reviews with an average rating of 4.4 stars;

- **G002**: it's a puzzle game where you have to move some boxes. The purpose is to make them explode in a determined number of moves. It has been downloaded 5 million times and it has 147,217 ratings and reviews with an average rating of 3.6 stars;

- **L002**: this app gives us the opportunity to modify the original lock screen with different themes. It has been downloaded 100,000 times and it has 929 ratings and reviews with an average rating of 3.9 stars;

- **G003**: the user has a maximum time to shoot more birds possible. It has been downloaded 1 million times and it has 9,418 ratings and reviews with an average rating of 3.8 stars;

- **A001**: this app has the purpose of transforming user's smartphone in a BitCoin miner. The user has one hour to try it and after he has to pay. It has been downloaded 50,000 times and it has 804 ratings and reviews with an average rating of 3.2 stars;

- **A002**: using this app the user has the opportunity to download applications not present in the official store. It has been downloaded 10,000 times and it has 167 ratings and reviews with an average rating of 3.8 stars;

- **U001**: useful to use the smartphone like a torch. The user can turn on and off the flash. It has been downloaded 50 million times and it has 1,157,657 ratings and reviews with an average rating of 4.7 stars;

- **A003**: the user can register meals and the app shows when user exaggerates. The purpose is to help you lose weight even through some diets. It has been downloaded 10 million times and it has 735,978 ratings and reviews with an average rating of 4.7 stars;

- **U002**: it's a widget with cigarette form. This cigarette consumes itself every time the battery charge decreases. It has been downloaded 1 million times and it has 22,881 ratings and reviews with an average rating of 3.9 stars;

- **M001**: this app has the purpose of enriching our SMS with emoticons and images. It also allows you to highlight some messages and gives you the opportunity to set a password for some texts. It has been downloaded 50 million times and it has 1,609,489 ratings and reviews with an average rating of 4.4 stars;

- **A004**: by this app a user can choose to share some backgrounds or to vote and download other users backgrounds. It has been downloaded 10 million times and it has 347,013 ratings and reviews

with an average rating of 4.3 stars;

- **M002**: it's a simple chat application. It has been downloaded 100,000 times and it has 431 ratings and reviews with an average rating of 3.3 stars;

- **G004**: the purpose of this game is to throw objects to a virtual colleague and realize more points possible. It has been downloaded 5 million times and it has 70,954 ratings and reviews with an average rating of 3.7 stars;

- **V001**: it's a database of sexy videos for adult. It has been downloaded 10 million times and it has 169 ratings and reviews with an average rating of 4 stars;

- **G005**: it's a puzzle game where the user has to combine three or more aliens of the same colors to increase his score. It has been downloaded 1 million times and it has 5,905 ratings and reviews with an average rating of 4 stars;

- **G006**: the user has to play beach-volley using the famous worms of the game Worms. It has been downloaded 1 million times and it has 37,939 ratings and reviews with an average rating of 3.7 stars;

- **G007**: the user has to think to someone (popular or not) and the genius guesses who is. It has been downloaded 10 million times and it has 277,529 ratings and reviews with an average rating of 4.2 stars;

- **G008**: save the elderly woman helping her avoid the obstacles. It has been downloaded 10 million times and it has 474,215 ratings and reviews with an average rating of 4.2 stars;

- **G009**: the user has to move some icons to redial the image seen at the beginning. It has been downloaded 5,000 times and it has 96 ratings and reviews with an average rating of 3.6 stars;

- **G010**: the user must use a slingshot to shot birds against the pigs in the castle. It has been downloaded 100 million times and it has 3,182,671 ratings and reviews with an average rating of 4.4 stars;

- **A005**: this app provides some backgrounds. For some backgrounds the user must pay and for others the user must not. It has been downloaded 10 million times and it has 1,166,212 ratings and reviews with an average rating of 4.7 stars;

- **U003**: with this app you can read the bar code of each product and search directly on the web some details of it. It has been downloaded

100 million times and it has 630,083 ratings and reviews with an average rating of 4.1 stars;

- **M003**: it's an app created to connect iPhone users and Android users with Blackberry users. It has been downloaded 50 million times and it has 1,951,368 ratings and reviews with an average rating of 4.2 stars;

- **G011**: by this game the user can play at Chinese chess in "one player" mode. It has been downloaded 100,000 times and it has 2,203 ratings and reviews with an average rating of 3.6 stars;

- **G012**: it's a strategy war game with a beautiful graphics. It seems that the game uses the IMEI for the user's login. When we have started to play, the game log us with an account at a high level. Probably someone has played it through the vm[12]. For real devices there is no account problem. It has been downloaded 1 million times and it has 41,806 ratings and reviews with an average rating of 4 stars;

- **U004**: it's an antivirus. It has been downloaded 50 million times and it has 4,742,303 ratings and reviews with an average rating of 4.7 stars;

[12] The IMEI of the virtual machine is 0000000000000000. If another user has played the game through a vm, probably it had the same IMEI.

- **M004**: send messages, images and voice notes to your friends. It has been downloaded 50,000 times and it has 135 ratings and reviews with an average rating of 4.4 stars;

- **U005**: if you have lost your smartphone this app could help you find it. If another device gives you the opportunity to find it, you can know even the location of it. It has been downloaded 10 million times and it has 96,198 ratings and reviews with an average rating of 4.2 stars;

- **G013**: the user has to use his finger to touch the screen and make leap the main character to avoid obstacles. It has been downloaded 10 million times and it has 841,752 ratings and reviews with an average rating of 4.4 stars;

- **U006**: this app is useful to make small changes to the lock screen. It has been downloaded 50 million times and it has 829,616 ratings and reviews with an average rating of 4.4 stars;

- **A006**: a collection of guides for the famous game Flappy Bird. It has been downloaded 100,000 times and it has 1,419 ratings and reviews with an average rating of 3.3 stars;

- **D002**: through this application it's possible to download music from a database made available by the developers. It has been downloaded 100 times and it has 2 ratings and reviews with an average rating of 5 stars;

- **A007**: this app offers a collection of guides on how to become a hacker. It has been downloaded 500,000 times and it has 7,633 ratings and reviews with an average rating of 4.2 stars;

- **U007**: through this app, the user can manage his finances. He can register all the money spent and earned and there is the possibility to create some graphs. It has been downloaded 50,000 times and it has 1,580 ratings and reviews with an average rating of 4.4 stars;

- **A008**: this app gives us the opportunity to enter in a device of someone near us. Really, this app is just a joke to tease your friends. It has been downloaded 10,000 times and it has 243 ratings and reviews with an average rating of 3.6 stars;

- **G014**: in this game the purpose is to shoot to some evil birds. It has been downloaded 500,000 times and it has 4,221 ratings and reviews with an average rating of 4 stars;

- **V002**: the purpose of this application is to share videos with your friends in high definition. It has been downloaded 5 million times and it has 16,047 ratings and reviews with an average rating of 3.5 stars;

- **M005**: it seems to be a social network, but indeed it's a chat application where you can talk with people that you don't know. It has been downloaded 1 million times and it has 94,079 ratings and reviews with an average rating of 4.2 stars;

- **G015**: each user challenges another random user. To win is necessary to find more words than your opponent in the shortest possible time. It has been downloaded 10 million times and it has 185,901 ratings and reviews with an average rating of 4.2 stars;

- **G016**: the purpose is to finish the motocross circuit in the shortest time. It has been downloaded 1 million times and it has 5.680 ratings and reviews with an average rating of 3.6 stars;

- **G017**: in this game the user has to hit PSY (a famous Korean singer) during the show on the stage. It has been downloaded 500,000 times and it has 5,044 ratings and reviews with an average rating of 3.8 stars;

- **G018**: the aim is to save the main character from the monsters that chase him. It has been downloaded 100 million times and it has 3,218,231 ratings and reviews with an average rating of 4.3 stars;

- **D003**: through this app the user can download all the videos found on the web. It has been downloaded 1 million times and it has 22,393 ratings and reviews with an average rating of 3.9 stars;

- **M006**: this app allows you to send messages using the internet connection of the device. It has been downloaded more than 500 million times and it has 17,533,412 ratings and reviews with an average rating of 4.4 stars;

- **A009**: this app simulates the use of a lighter. It has been downloaded 10 million times and it has 66,834 ratings and reviews with an average rating of 4.1 stars;

- **M007**: it's not a very app to send messages. The user can use this app to create images with a text to send using another app. It has been downloaded 500,000 times and it has 2,013 ratings and reviews with an average rating of 2.7 stars;

- **A010**: through this app is possible to recognize the title and the author of the song that is transmitted near the user. It has been

downloaded more than 100 million times and it has 1,604,265 ratings and reviews with an average rating of 4.4 stars;

- **G019**: tap the screen and avoid obstacles with your dog. It has been downloaded 1 million times and it has 44,321 ratings and reviews with an average rating of 4.2 stars;

- **A011**: the purpose of this app is to promote other applications. It has been downloaded more than 1 million times and it has 49,743 ratings and reviews with an average rating of 4.3 stars;

- **G020**: avoid other cars and save your car for much time as possible. It has been downloaded 10,000 times and it has 538 ratings and reviews with an average rating of 3.5 stars;

- **G021**: the user has to shot some enemies. It has been downloaded 100,000 times and it has 1,383 ratings and reviews with an average rating of 3.4 stars;

- **U008**: through this application the user can send to a friend one or more help messages. It has been downloaded 5,000 times and it has 158 ratings and reviews with an average rating of 4 stars;

- **S002**: it's a social network with the aim to meet new friends. It has been downloaded 50,000 times and it has 653 ratings and reviews with an average rating of 3.6 stars;

- **S003**: through this social network you can partecipate to random chat and random discussion. It has been downloaded 5 million times and it has 124,462 ratings and reviews with an average rating of 3.9 stars;

- **S004**: it's very similar to a dating website. It has been downloaded 50,000 times and it has 1,281 ratings and reviews with an average rating of 3.8 stars;

- **S005**: in this social network you can see only girl if you are a man and vice versa. It has been downloaded 5 million times and it has 169,724 ratings and reviews with an average rating of 4.1 stars;

- **S006**: very useful to know new people who live near you. It has been downloaded 1 million times and it has 88,084 ratings and reviews with an average rating of 4.4 stars.

We have assigned to each application a code name and a synthesis. In this way the reader could understand that the applications selected are normal apps and probably he can also recognize them.

The applications listed are in the same order in which they were downloaded and tested. As you can see, we have tested applications usually downloaded to work, or to play, or to have fun, or to share something. For each applications we have reported the number of downloads, the number of ratings and reviews and the average rating.

At this point we want to discover if the applications chosen are safe or unsafe. An application is safe when we cannot assign to it no level of danger. An application is unsafe when we can assign to it one level of danger.

4.1.2 Safe and Unsafe Applications

Following the protocol described on the third chapter we have tested all the applications listed before and we have assigned to each app a level of danger. Now we have to see some statistics based on safe and unsafe apps.

We remember that we have a total of 60 applications tested. All the apps have been downloaded from Google Play Store.

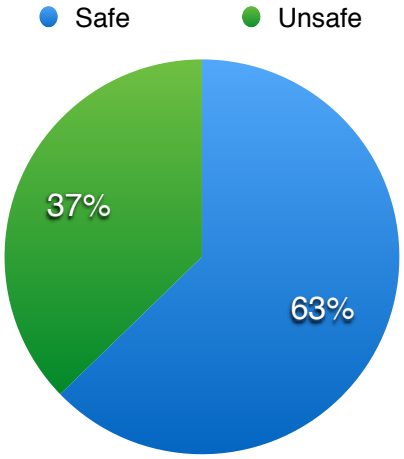

Figure 4.1: The pie chart shows us the ratio between safe and unsafe applications in the Play Store.

As we can see, the percentage of unsafe applications is not very low. The 37% of the applications tested present a suspicious behaviour and this is not a good news. However, we have to discover how the level of danger is distributed between these unsafe apps.

We have created a new pie chart that shows us the percentage of presence of each danger level. As seen above, each level of danger is represented by one or more exclamation points (more exclamation points we assigned to an application and more the app is unsafe).

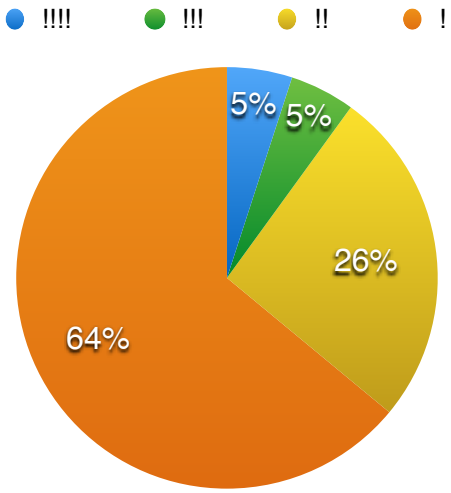

Figure 4.2: The pie chart shows us the presence of each level of danger assigned to one or more apps.

Fortunately, a great percentage of unsafe applications has assigned the first level of danger. However, the percentage in respect of the third

and the fourth level of danger is not negligible. An application that has assigned four or three exclamation points it's really unsafe for the privacy of the users and even for the security of the devices.

Let's pretend that the Google Play Store has precisely 1 million apps uploaded. Assuming that the sample is representative of the entire universe, we could say that 370000 of these applications are not safe and precisely 37000 applications have a high level of danger (three or more exclamation points). As we have written in chapter 1, in 2013 the Google Play Store had 42000 unsafe applications [12], so these statistics are very realistic.

The next step is to show some examples of unsafe apps for each level of danger. After that, we will be ready for permissions statistics.

4.1.3 Examples of Unsafe Applications

Up to this moment we have introduced the levels of danger that teach us vaguely how much an application can be unsafe. The best way to explain to the reader why an app has assigned one, two or more exclamation points, is to show him some examples.

!!!!. One of the applications that has assigned four exclamation points is an app that permits the download of the videos on the web (we have described it with code name D001). This app drew our attention because of the required permissions that now we list:

- **Storage**: modify or delete content of your Secure Digital (SD) card;
- **System tools**: modify system settings, prevent phone from sleeping;
- **Your location**: approximate (network-based) location;
- **Network communication**: full network access;
- **Your personal information**: read your web bookmarks and history, write web bookmarks and history;
- **System tools**: run at startup;
- **Network communication**: download files without notification, view Wi-Fi connections, view network connections;
- **Development tools**: test access to protected storage;
- **Your accounts**: find accounts on the device.

This application required some strong permissions that even the reader with less experience notices that it's better to not download it. For example, one of the permissions which has aroused more curiosity in us is the second "Network communication" in the list. It says that this app may download files without any notification. If the reader takes a look to all permissions, it's not difficult to discover that this app could be unsafe. It could download a file to be executed on startup to access protected storage, or to write bookmarks, or to delete the content of the SD card, etc.

However, we have executed this application in our virtual machine and we discovered that, first of all, it tries to localize us, to know if there is a microphone and what's the language on our vm. After that, this app has some preset platforms for the video sharing. So, we have selected YouTube and even before that we make the first research it asks us to download and install Adobe Flash Player[13] [24].

This software is no longer installed in any device [26]. Moreover, our virtual device can execute all the videos present on YouTube without an external download. Obviously the reader doesn't have to download and install this kind of file. For our purpose we have decided to download and install it. The download starts without going through the Play Store and the app wants that we open settings and that we give the consent to install app from unknown sources. Obviously this application has already violated all the standards written by Google. First of all, an app that recommends another application guides the user through the Play Store

[13] It's a freeware software for viewing multimedia, executing rich Internet applications and streaming video and audio [25].

to download it. Secondly, only for the development a user has to give the consent to unknown sources (during the development an app is not signed).

Anyway, we have downloaded and installed it discovering from where we took this file. Using *ipaddress.com* we have discovered that we have downloaded it from a server of the Akamai Technologies, an agency that offers sharing services and mirroring services. It's very important to discover that this file isn't downloaded from the Play Store and neither from the official website of Adobe.

At this point, moving through the menu, we have found the icon of the app downloaded. We have tried to start the app, but nothing happened. Using the app D001, through Wireshark we can see that the app wants to search and download a video called "Video Meeting Date Download" that we have never searched. We have not found this video on the virtual device, anyway we are sure that this is not a safe application.

This app has been downloaded 10 million times and has an average rating of 4 stars.

!!!. One of the applications that has three exclamation points is S001. This application seems something like Facebook, but tries to find for you some possible colleagues (like LinkedIn) and at the same time suggests to you some girls (like a dating website). Even this app drew our attention because of the required permissions (this particular should

make it clear to the reader that permissions are very important to recognize unsafe apps). So, the permissions required are:

- **Storage**: modify or delete the contents of your SD card;
- **Your messages**: read your text messages (SMS or MMS);
- **System tools**: change system display settings, connect and disconnect from Wi-Fi, retrieve running apps;
- **Your location**: approximate (network-based) location, precise (GPS) location;
- **Phone calls**: read phone status and identity;
- **Network communication**: full network access;
- **Your personal information**: read your web bookmarks and history, read your contacts;
- **System tools**: run at startup;
- **Development tools**: test access to protected storage;

- **Your location**: access extra location provider commands;
- **Hardware controls**: control vibration;
- **Network communication**: view Wi-Fi connections, view network connections.

This application required strong permissions like “Your personal information” and “Your messages”. Even this time a careful user can understand that this app is not safe. Let’s get the perspective of the user who wants to enter in a new social network and chooses to download S001. If he reads the permissions, he could immediately understand that a social network doesn’t need to read user’s SMS and MMS and other data like bookmarks and history from the browsers installed.

However we have downloaded and tested this app to discover what it really does. So, we have started the app and immediately it has read the IMEI code. After that, it requires to register and to give the phone number and one password. As soon as we write the phone number, we can see through Wireshark that the app takes the number and send it to its servers. At this point, we write the password, the name and the date of birth. Finished the registration we see all these data go to the app servers. The wrong thing resides in the fact that all these data are sent without a form of encryption. Whoever is sniffing the network when a

user puts his data in the registration form could see user's password, phone number, name and the date of birth.

At this point, S001 activates the GPS and says that wants help us connect to the contacts in our address book that already use S001. So, this app really takes our contacts, but it takes even all the email addresses present in our account Hotmail, Google Mail (Gmail) and even the email addresses of the University of Bologna. Moreover, it takes for each browser the history and the bookmarks.

This application sends again all the data without a form of encryption. However, after the registration, the app said to us that it just wanted to search in our address book if someone was already a member of the social network, but really it took a lot of things that are not useful for the application. For example, S001 doesn't do anything with our bookmarks and history and the same thing is for our SMS that probably it cannot take because we don't have a SIM card.

```
0370  25 32 43 76 65 72 6e 61  2e 74 68 65 62 65 73 74   %2Cverna .thebest
0380  25 34 30 68 6f 74 6d 61  69 6c 2e 69 74 25 32 43   %40hotma il.it%2C
0390  76 65 72 6e 61 2e 74 68  65 62 65 73 74 25 34 30   verna.th ebest%40
03a0  68 6f 74 6d 61 69 6c 2e  69 74 25 32 43 25 32 43   hotmail. it%2C%2C
03b0  30 25 33 42 31 34 25 32  43 67 69 6f 76 69 2d 70   0%3B14%2 Cgiovi-p
03c0  61 74 6f 25 34 30 68 6f  74 6d 61 69 6c 2e 69 74   ato%40ho tmail.it
03d0  25 32 43 67 69 6f 76 69  2d 70 61 74 6f 25 34 30   %2Cgiovi -pato%40
03e0  68 6f 74 6d 61 69 6c 2e  69 74 25 32 43 25 32 43   hotmail. it%2C%2C
03f0  30 25 33 42 31 35 25 32  43 65 6e 67 69 32 25 34   0%3B15%2 Cengi2%4
0400  30 6c 69 62 65 72 6f 2e  69 74 25 32 43 65 6e 67   0libero. it%2Ceng
0410  69 32 25 34 30 6c 69 62  65 72 6f 2e 69 74 25 32   i2%40lib ero.it%2
0420  43 25 32 43 30 25 33 42  31 36 25 32 43 4d 69 63   C%2C0%3B 16%2CMic
0430  68 65 6c 65 25 32 43 6d  69 6b 65 6c 65 2e 76 61   hele%2Cm ikele.va
0440  6c 65 6e 74 69 25 34 30  67 6d 61 69 6c 2e 63 6f   lenti%40 gmail.co
0450  6d 25 32 43 25 32 43 30  25 33 42 31 37 25 32 43   m%2C%2C0 %3B17%2C
0460  41 6c 65 73 73 69 6f 2b  49 72 6c 61 6e 74 65 25   Alessio+ Irlante%
0470  32 43 56 69 72 6c 61 6e  74 25 34 30 68 6f 74 6d   2CVirlan t%40hotm
0480  61 69 6c 2e 69 74 25 32  43 25 32 43 30 25 33 42   ail.it%2 C%2C0%3B
0490  31 38 25 32 43 4d 61 6e  75 65 6c 61 2b 53 63 75   18%2CMan uela+Scu
04a0  64 65 72 69 25 32 43 6d  61 6e 75 65 6c 61 25 34   deri%2Cm anuela%4
04b0  30 6e 65 77 6d 65 64 69  61 62 69 74 2e 69 74 25   0newmedi abit.it%
```

Figure 4.3: A piece of a Wireshark capture file. The app takes the email addresses of some friends.

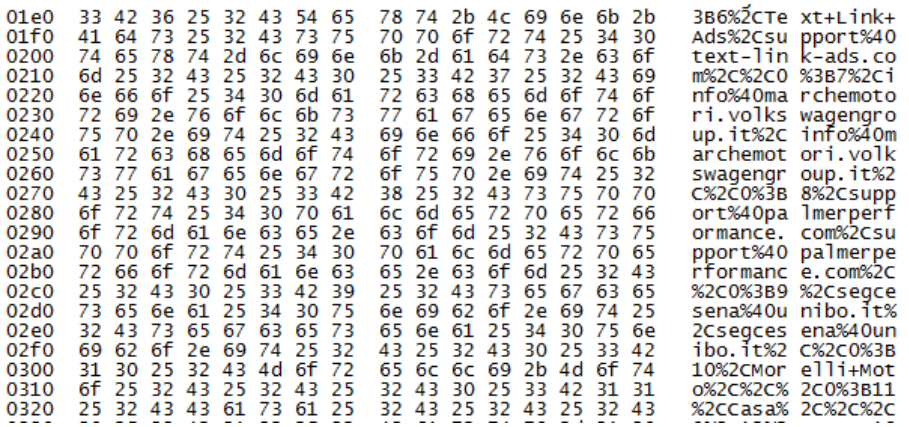

Figure 4.4: A piece of a Wireshark capture file. The app takes our bookmarks.

We have always checked who owns the IP addresses found because we know that often some agencies collect data to sell to other companies. Using ipaddress.com we have searched some IP finding that all this data mentioned were sent to an advertizing agency that resides in Beijing.

At the end, we have checked if new processes or apps were started. We have found the application for the management of the emails and the process “Bookmarks”. Previously they weren’t open.

This application has been downloaded 10000 times with an average rating of 4.3 stars.

Regarding two and one exclamation points we have more examples, but we would be repetitive because these applications do approximately some of the already seen things. For example, we have a “two-exclamation-points” application, L001, that takes the IMEI of the virtual

device, the IP and some other things like the network-based position. Another example, we have an “one-exclamation-point” app, L002, that tries to activate the GPS without a known purpose.

4.1.4 Permissions

When a developer needs to take some important data or to use some particular tools like the camera, he has to declare the appropriate permissions in the manifest file of the application. The manifest file is bundled into the Android installation package file. It provides all the necessary information to the Android platform for the execution of the application [10]. It’s not possible for a user to install an application that doesn’t declare the right permissions and it’s a merit.

First of all, permissions give to the users the possibility to know what sensible data and what sensible actions the application could do. Secondly, permissions give to the system the possibility to know what resources it needs to execute the app. As we have seen above when we have listed the permissions required by the two unsafe applications, permissions are related to accounts on device, system tools, personal information, location, hardware controls and to all the other things that an attacker could exploit to harm the privacy of the users or the devices.

We show now all the permissions required by the unsafe applications tested with the purpose to understand what permissions, if required together, can be dangerous for users or for devices.

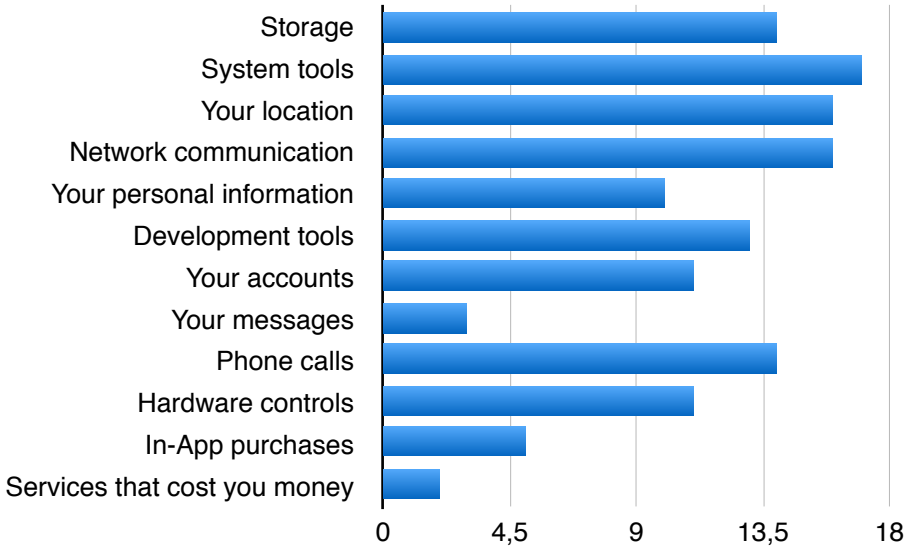

Figure 4.5: Histogram about the permissions required by all the unsafe applications.

Through this histogram is possible to understand that many applications required permissions like “System tools”, “Your location” and “Network communication”. These permissions are often required and for this reason doesn’t help us understand if an application is really unsafe. Obviously, when an app has the possibility to be connected to the Internet, send our location data to other services it’s a privacy threat. Today, all the advertising agencies require the location to send the localized advertising.

Looking at the histogram is possible to see that there are some permissions like “Services that cost you money”, “Your messages” and “Your personal information” that are less required. These permissions are very dangerous. As we have seen before, the application S001 requires

two of these three permissions. When we were searching applications we have immediately noticed that the permissions required by S001 are not safe permissions. For our purpose, we have downloaded the app even if, without knowing the application, we had some suspects. Permissions like “Your messages” give the possibility to read the content of all of the messages present on the device. Furthermore, it can give even the possibility to write some SMS and MMS. Thinking to the nature of S001, is inexplicable to understand why a social network application could use safely this permission. We can make the same reasoning for “Your personal information”. Even this time, it’s not really full of meaning. An app like S001 doesn’t need to read bookmarks and history of our browsers.

After reading this chapter, the reader could think that all the applications which require these permissions are unsafe. It’s not true. For example, thinking on an application that requires permissions like “Services that cost you money” and “Your messages”. If we know that this application has the purpose to send SMS, we don’t have to be suspicious. The application may even send strange SMS without your consent, but if many users think that is a great app, we can almost trust. If, contrariwise, we want to download a game and it requires permissions like “Your messages”, we have to think about this chapter and we cannot trust.

One of the most important permissions for the privacy threat is “Network communication”. This permission is very important because

application like the one of the first example cannot do anything to undermine our privacy without a connection to the Internet. The app could be unsafe because writes SMS without our consent or because sends messages with our privacy data to strange numbers, but the user could uninstall the app as soon as he notices it. With the “Network communication” permission, the network activity is not visible to the user. So, the app could take, in less time, all the messages and could send them to its servers.

As we will see in the next chapter, our purpose is to teach the reader to recognize malware and privacy threats simply by reading the permissions.

4.2 iOS Analysis

Regarding iOS, we have to give for each application a code name and a synthesis. After that, we will show some statistics and some examples.

4.2.1 iOS Code Names

We have used the same way viewed for Android to assign the code name to each application. To recognize the iOS applications from the Android applications we have put in front of the iOS code name the letter “i”. This is the list of the applications tested:

- **iA001**: this application permits to see all the charts and the quotes of all the different virtual coins (like BitCoin, DogeCoin, etc.). It has 16 ratings and reviews with an average rating of 4 stars;

- **iG001**: the user has to guess in which point place the explosive. It has 81 ratings and reviews with an average rating of 4.5 stars;

- **iG002**: the user may create some virtual Mexican tacos and he can share it on Facebook. It has 36 ratings and reviews with an average rating of 3.5 stars;

- **iU001**: through this application the user has the possibility to manage his finances. It has 0 ratings and reviews with an average rating of 0 stars;

- **iG003**: it's a football game where the user uses a virtual joystick to play with some stylized characters. It has 707 ratings and reviews with an average rating of 4 stars;

- **iA002**: guess who is the wrestler in the blurry photo. It has 19 ratings and reviews with an average rating of 4 stars;

- **iG004**: it's a game of logic where the user has to understand how to have access to a network or a PC. It has 0 ratings and reviews with an average rating of 0 stars;

- **iG005**: it's a copy of the famous Snake presents in the old Nokia phones. It has 321 ratings and reviews with an average rating of 3.5 stars;

- **iG006**: it's a game like Super Mario Bros, but the main character is a rabbit. It has 0 ratings and reviews with an average rating of 0 stars;

- **iG007**: save the chicks making them fly with the best trajectory to the finish. It has 2 ratings and reviews with an average rating of 5 stars;

- **iG008**: the user has to tap on the screen with the purpose to save the soldier with his Jet-Pack. It has 5 ratings and reviews with an average rating of 4 stars;

- **iA003**: it's not a very intuitive app. The purpose is to write notes and attach photos. It has 0 ratings and reviews with an average rating of 0 stars;

- **iU002**: this application is useful to record a singer and the audio recorded is very clean. It has 314 ratings and reviews with an average rating of 4 stars;

- **iG009**: the user has to move the animals with the same color to combine some tris. It has 309 ratings and reviews with an average rating of 4.5 stars;

- **iS001**: a new social network where a user has to share his location. More places the user submits and more points he acquires. It has 400 ratings and reviews with an average rating of 4 stars;

- **iG010**: you have to move a monster through three or more points without go through the same points more than one time. It has 3 ratings and reviews with an average rating of 4 stars;

- **iA004**: through this application you can improve math and especially the math fractions. It has 2 ratings and reviews with an average rating of 5 stars;

- **iG011**: the user must build a beautiful farm. It has 1,167 ratings and reviews with an average rating of 4 stars;

- **iA005**: it's for a female audience. This app teaches you some exercises to have a perfect body. It has 10 ratings and reviews with an average rating of 3.5 stars;

- **iA006**: this app shows to the user some random numbers to use for a bet or something similar. It has 6 ratings and reviews with an average rating of 3 stars;

- **iA007**: this application collects all the medicines present on the market and for each medicine gives some information. It has 72 ratings and reviews with an average rating of 4 stars;

- **iG012**: it's the solitaire game. It has 11.022 ratings and reviews with an average rating of 4.5 stars;

- **iA008**: this app is updated with all the new sticker albums. The user can choose to write notes about some stickers, if he doesn't have it or if he has it twice. It has 0 ratings and reviews with an average rating of 0 stars;

- **iA009**: the user can play the virtual triangle. It has 21 ratings and reviews with an average rating of 2 stars;

- **iA010**: through some pencils, effects and filters the user can edit his images and photos. It has 28 ratings and reviews with an average rating of 4 stars;

- **iU003**: it's a calendar with the aim to organize user's work. It has 405 ratings and reviews with an average rating of 4.5 stars;

- **iA011**: this app has a database of sarcastic images to share on the social networks. It has 49 ratings and reviews with an average rating of 4.5 stars;

- **iA012**: this app is for A.C. Milan fans and it has many articles directly from Milan News. It has 3,629 ratings and reviews with an average rating of 4.5 stars;

- **iD001**: the user may listen to relax music and may download it. It has 2 ratings and reviews with an average rating of 4 stars;

- **iD002**: through this app a user could watch videos on YouTube and download them. It has 2 ratings and reviews with an average rating of 1 star;

- **iG013**: the user has to help a ninja that earns points fishing in a lake. It has 3,538 ratings and reviews with an average rating of 4.5 stars;

- **iS002**: it's very similar to Facebook. It permits to share your thought with friends and chat with them. It has 2,214 ratings and reviews with an average rating of 4.5 stars;

- **iA013**: this app is useful for parents who want to teach prayers to their sons. It has 215 ratings and reviews with an average rating of 4 stars;

- **iG014**: guess who is the actor hidden behind the black silhouette. It has 22 ratings and reviews with an average rating of 4 stars;

- **iA014**: it's an application that teaches users to do yoga. It has 224 ratings and reviews with an average rating of 2.5 stars;

- **iA015**: this application helps the student that wants to solve algebraic expressions. It has 129 ratings and reviews with an average rating of 4 stars;

- **iG015**: move the robot in the hockey match and win. It has 0 ratings and reviews with an average rating of 0 stars;

- **iG016**: it's a game identical to the famous Flappy Bird. It has 5 ratings and reviews with an average rating of 3 stars;

- **iA016**: you can choose the best cover for iPhone and buy it. It has 161 ratings and reviews with an average rating of 4.5 stars;

- **iU004**: it's not a normal shopping list. The best thing is that you can share the shopping list with your family and your relatives can add something to the list. It has 1,771 ratings and reviews with an average rating of 4.5 stars;

- **iG017**: find the differences between two images or photos. It has 175 ratings and reviews with an average rating of 4 stars;

- **iG018**: place your defenses on the right boxes to stop the enemy advance. It has 27 ratings and reviews with an average rating of 3.5 stars;

- **iA017**: this app promises to guess if the user says the true. It has 19 ratings and reviews with an average rating of 3.5 stars;

- **iA018**: this application shows all the news of the Catholic Church and where are the principle places of worship. It has 33 ratings and reviews with an average rating of 4.5 stars;

- **iD003**: this app permits to download the videos present on YouTube. It has 61 ratings and reviews with an average rating of 4 stars;

- **iS003**: it's a Japanese social network with only Japanese users. It has 0 ratings and reviews with an average rating of 0 stars;

- **iG019**: guess the words hidden in the mixed letters. It has 5 ratings and reviews with an average rating of 4 stars;

- **iS004**: it seems like LinkedIn with a great number of users from Asia. It has 6 ratings and reviews with an average rating of 4 stars;

- **iA019**: if you are in a new place and you don't know where to eat, or to sleep, etc. this application will show you the nearest places you need. It has 658 ratings and reviews with an average rating of 3.5 stars;

- **iG020**: it's like the famous Pinball, but it has beautiful graphics. It has 687 ratings and reviews with an average rating of 4 stars;

- **iG021**: it's a game to have fun with your girlfriend. It has 136 ratings and reviews with an average rating of 4 stars;

- **iG022**: help a donut to complete a lap on a circuit. It has 125 ratings and reviews with an average rating of 4.5 stars;

- **iA020**: the user can choose one gun and shoot with the aim to listen the sound of the shot. It has 427 ratings and reviews with an average rating of 4.5 stars;

- **iS005**: it's a social network where you can meet your new flame. It has 2,234 ratings and reviews with an average rating of 4.5 stars;

- **iG023**: tap the screen and avoid obstacles with the copter. It has 918 ratings and reviews with an average rating of 3.5 stars;

- **iA021**: watch the lake with some fish and change the environment as you want. It has 3 ratings and reviews with an average rating of 4 stars;

- **iG024**: combines the stones and complete some tris. It has 0 ratings and reviews with an average rating of 0 stars;

- **iG025**: dress the girls and make up their faces. It has 0 ratings and reviews with an average rating of 0 stars;

- **iS006**: share some photos of your pets with other users. It has 5 ratings and reviews with an average rating of 4 stars;

- **iA022**: through this application the users have the possibility to buy some health-care products. It has 55 ratings and reviews with an average rating of 4.5 stars.

4.2.2 Safe and Unsafe Applications

All the applications tested have been chosen like for the Android case, but without checking permissions. However, we have assigned a level of danger to each application and even a code name and a synthesis. We have tested 60 iOS applications.

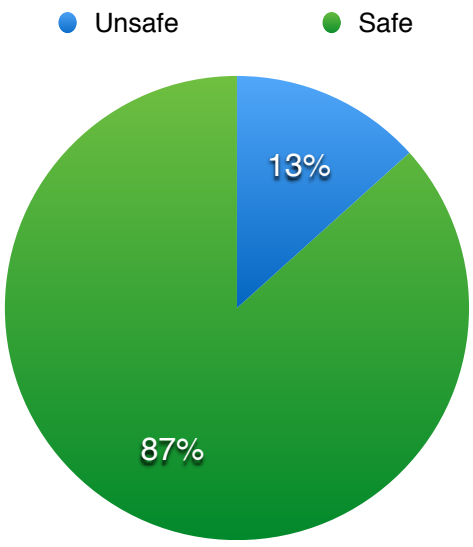

Figure 4.6: The pie chart shows us the ratio between safe and unsafe applications in the Apple App Store.

The situation is a bit different from Play Store for Android. In this case, only the 13% of the applications tested are unsafe (while for Play Store the 37% of the applications are unsafe).

So, we have created a new pie chart that represents in which way the levels of danger are distributed through the unsafe applications. Even this time, we will use the exclamation points to represent each level of danger.

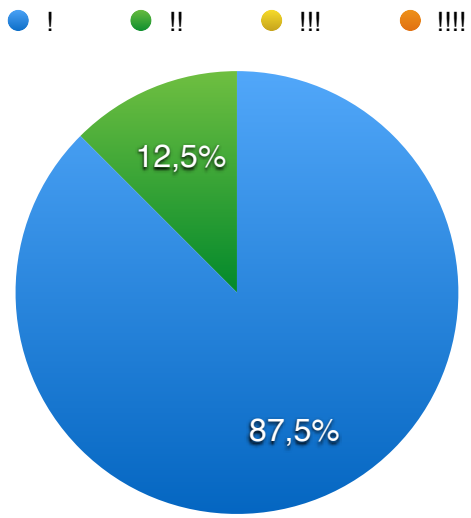

Figure 4.7: The pie chart shows us the presence of each level of danger assigned to no one, one or more apps.

Almost unexpectedly, all the unsafe applications have a low level of danger: these apps have a maximum of two exclamation points.

Assuming that the sample is representative of the entire universe and assuming that in the Apple App Store there are 1 million apps, probably 130000 are unsafe (for Android 370000). We don't have found applications like those seen for Android, but this is not a proof that

Apple App Store is more secure. In the sixth chapter we will try to draw conclusions on what is the safer store.

4.3 Summary

In this chapter we have seen firstly the Android analysis phase. We have found some unsafe applications and especially some of these apps are of a high level of danger. We have showed some statistics about the Play Store and the ratio between safe and unsafe applications. At this point, the chapter has focused on what some unsafe apps do to be unsafe. After that, the reader could see some statistics on permissions required by the unsafe applications.

Regarding iOS, we have showed the same things except for permissions. Unexpectedly only the 13% of the apps tested are unsafe and all these unsafe applications have assigned a maximum of two exclamation points.

In the next chapters we will see why it couldn't be true that the Apple App Store is more secure than Google Play Store. For now, we can only say that there is the possibility to have chosen more unsafe apps for Android for chance. In addition, we can also say that permissions could have conditioned our choice in Android tests, but at the same time the user could avoid downloading unsafe applications just reading permissions.

Chapter 5

Security Steps for Users

This chapter focuses on what are the security steps that a user of mobile devices should follow. These security steps are not the solution, but they can be the best way to avoid downloading privacy threats and malware. In this chapter we describe what's the role of the user about permissions, system updates and antiviruses.

5.1 Read the Permissions

In the previous chapters we have already underlined the importance of reading permissions. As we know, when an Android user wants to download an application, the Play Store puts in front of him the permissions that the app required. These permissions are really important. In this way both the user and the system knows what kind of

actions the app could do. The only problem is that, while the system reads truly these permissions, the users often do not.

Let's think about the application with three exclamation points mentioned in the previous chapter. We remember that the permissions required by S001 were a clear signal of the real intention of the application. The permission required that really doesn't have a meaning is "Your personal information: read your web bookmarks and history, read your contacts". A careful user probably can understand that a social network app doesn't need to read bookmarks and history. The main thing that all the users must understand is that it's important to be careful. Just reading permissions, users can avoid downloading a lot of malicious applications. Unfortunately, in the real world users don't pay much attention to permissions and they often don't understand them [27]. Our advice is to document yourself on the meaning of each permission and especially to download almost exclusively apps with a known goal. If you know what the application must do to achieve the target, you understand better the permissions and, at the same time, you know if a permission is or not necessary. If you don't know what's the goal of the application, you must pay some attention on its description trying to understand if it's safe or not. At the end, you cannot trust about votes and reviews of other users or friends because probably many of them don't have read the permissions.

5.1.1 Some Tips for Google

We think that Google cares about the security of his market, so we think that it could do something to change the situation. First of all, Google should try to improve the virus search within the Play Store. After that, Google should persuade the users to read all the permissions. The way to follow is to oblige the users to accept each permission required. In this way, if a user wants to download an application that required twenty permissions, he has to click on “Accept” twenty times and probably his attention falls on each permission. Finally, Google should give the possibility to the user to deny one or more permissions. In this case, Google should replace missing data of the app with standard data. We really think that permissions could teach the users to be careful and to understand how to recognize a malware or a privacy threat using their brains.

5.2 Antivirus

Another way to avoid downloading malware and privacy threats is to download antiviruses. We have found a lot of antiviruses for Android and just one antivirus for iOS. We think that this scenario occurs because iOS users trust more the security mechanisms adopted by Apple. However, antiviruses for mobile devices are not very used [28]. First of all, users think that is unnecessary to download antiviruses for smartphones

and tablets. This because they think that there is a great inspection of the applications in the respective stores. Secondly, the antiviruses for mobile platforms have not yet reached the same potential of the antiviruses for personal computers. Antiviruses for personal computers are very “heavy” and they often update their databases with new information on malware and privacy threats. Regarding mobile devices, it’s impossible to reproduce the same scenario. For example, an antivirus cannot overcome the size of 50 megabytes (MB). The reason is that in the Google Play Store a developer cannot upload an application with a size major of 50 MB [29]. A lot of low-level smartphones don’t have enough space for an antivirus. Moreover, updating the databases could be very expensive for the battery consumption, the use of the connection and even, later in time, for the memory of a high-level device. At the end, if we want an antivirus like those for the PC it means that the antivirus has to check for malware, spyware and trojan in each moment and this is a problem for the battery life [30].

We have decided to test some antiviruses for Android platform knowing that even the most famous antivirus for PC has not a great reputation on mobile devices [6].

5.2.1 Statistics on Antiviruses

We have chosen to test four of the well-known antiviruses for personal computers on the Android virtual machine. All of these antiviruses are free to download, so the reader could try them himself. The antiviruses tested are:

- MCAFEE;
- AVAST - Mobile Security & Antivirus;
- Kaspersky - Internet Security;
- AVG - Antivirus Security - Free.

Now we see how many unsafe apps these antiviruses have found:

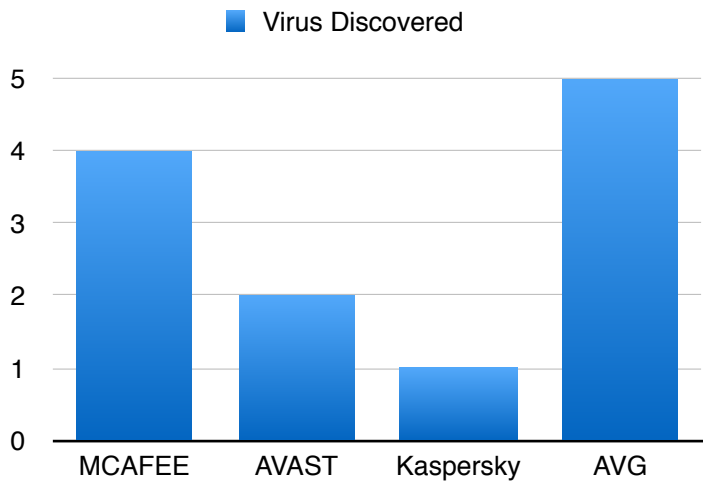

Figure 5.1: Histogram on the number of unsafe apps discovered by the four antiviruses tested.

It's very incredible to see that, on 22 malicious applications found by us through a scrupulous analysis, no antivirus finds at least ten applications. AVG, in this case, reveals to be the best antivirus with 5 unsafe applications found. In another scenario it could be different. AVG is even the only antivirus that has recognized S001 as a very unsafe application. This is very important because S001 is one of the most unsafe apps that we have tested. Moreover, it means that AVG is more updated and knows how to discover this kind of application.

Again we remember that this is not sufficient to know what is the best antivirus and is not our purpose to find it. Through this little analysis we know now that the antiviruses for mobile devices are not yet ready to protect our privacy and our devices.

5.3 Other Advice

The reader knows now the importance to read permissions and knows that could avoid downloading some unsafe applications using antiviruses. It's even more important to know that use the antivirus doesn't exclude to read permissions and vice versa. As we have seen above, the antiviruses are not ready to find all the malware and privacy threats present on the device. Furthermore, we have found more applications especially observing permissions and without use antiviruses.

Read permissions and use the antiviruses is not sufficient to protect user's data and devices. It's very important to update the smartphone OS

because, with the update, the developers could have implemented a new security mechanism. An example of a security mechanism that is gone unnoticed, it has been implemented by Apple, in fact in the old applications it was not necessary to inform the user on “when an app needs the GPS location, or to record audio, etc.” while now is required. We have reported this example because it’s a visible security mechanism to all the users. It’s simple, but at the same time is very efficient. However, let’s think to an unsafe application known to exploit an open port to take remote control of a device. When Google or Apple discovers it, it releases as soon as possible a system update to close the open port (for example). All the users that have not updated the system of their devices could be yet vulnerable to a remote control by a similar application.

Observing the last example, and thinking that through the remote control an attacker wants to delete all the user’s data, we recommend the users to backup their data quite frequently.

Users should not modify the OS files, they should not jailbreak the devices and take superuser privileges. This because, even if you could trust the source of an application that requires superuser privileges, you don’t know if there is another application that knows how to exploit its “power”.

5.4 Summary

Reading this chapter the reader should have understood that the task of avoid unsafe applications is of the user. Our smartphones and tablets are updated, when it's necessary, to improve the security mechanisms already present and to add new security mechanisms. Even antivirus companies are working to improve their software and to find a solution. We remember to the reader that an antivirus should be ever active and should have a database with a great number of information to discover unsafe applications. At the end, we have given some advice with the aim to have a more secure device. Update the device OS, backup all data and don't edit the OS files are already good advice.

To protect user's data and devices it's necessary a collaboration between the users, the application developers, the system owners and the antivirus agencies. The firsts have to read permissions, document themselves on the application to download, not modify OS files and use antiviruses. The seconds have to develop safe applications. Especially they have to take secure measures to ensure that no attacker can exploit buffer overflows, memory corruptions, open ports, etc. through their applications. The thirds have to implement more efficient security mechanisms and find a proper solution to battery life so that the antivirus companies can develop more efficient antiviruses. These companies should find a solution on "how to block a great percentage of unsafe apps".

In the next chapter we will illustrate to the reader who is better between iOS and Android even if, probably, we will not find a winner. The reader is free to choose what's the best.

Chapter 6

Android or iOS

Until now, we have illustrated the security mechanisms used by Android and iOS. We have shown our tests and analysis observing some unsafe applications and some statistics. At the end we have tried to give some advice to the reader and all the users of mobile devices. We have noticed that there are many unsafe applications for Android. The reader could think that, at this point, the solution is to choose iOS with no doubt. So, we will try now to make some reflections on Android and iOS and, at the end, the reader will be free to choose.

6.1 iOS

Regarding iOS, we have found that 13% of the applications tested are privacy threats of low-level entity. The system made by Apple seems to be more secure. When a developer submits an app in the App Store he has to wait some days to see his application published or to have a negative

response. iOS team wants that the application does the same things described in the description submitted. However, we think that it's not a good result the low number of unsafe applications discovered. The percentage of iOS unsafe apps is lower than the percentage of Android unsafe apps, but at the same time is curios to observe that without the opportunity to read permissions, or something like it, we have however found some unsafe applications. Honestly, thinking about the way in which we have searched the applications for Android, we really think that without reading permissions probably we would have a lower percentage of unsafe apps. Our task was to understand how are safe the two respective systems and especially the two respective stores. So, we have done our best to find the most dangerous application. Regarding iOS, without the possibility to read permissions, it's very difficult. The 13% of unsafe apps remembers to us that the App Store is not safe.

As developers, we can say that the App Store seems to be more controlled. At the same time, we cannot deny the fact that without reading permissions we have however found some unsafe apps.

Another thing that could scare the iOS users is the possibility to find some backdoors in iOS devices [31, 32]. We don't know for what these backdoors are present. However we know that, even if the reason is rational and reasonable, an attacker could find the backdoors and exploit them for his purposes.

Mainly, with the fingerprint reader to unlock the device, the often good research of unsafe applications and the low percentage of unsafe applications found by us, iOS with its App Store seems to be quite secure. Backdoors and some unsafe apps found remember to us that, anyhow, we cannot trust the Apple security mechanisms. We are trying to remain impartial because our purpose is to teach the users to never trust security mechanisms. Another example of an Apple problem on security mechanism happened in February 2014, when it has been discovered that there was a way to falsify the validation of the certificates on Secure Socket Layer (SSL) and Transport Layer Security (TLS) connection [33, 34].

At this point, the reader should have understood that iOS is not very secure, the same we will show for Android. At the same time, the reader should have understood that, if he wants a safe device, he has to execute some personal controls. Install only trusted and known apps, try to document himself on how much is safe an app, be careful on the battery consumption, etc. is always necessary. Unfortunately, there is no iOS security mechanism based on permissions. Permissions are always a good way to understand when an application is unsafe. Fortunately, on iOS systems the user is always felt on when an app needs to use connection, camera, GPS, etc. However, we have found some privacy threats, and we think that a user cannot accept a lot of alerts for IMEI, IP, accounts, MAC address, etc. So, it’s right to not report an alert for each thing, but

at the same time is not correct that a user doesn't know what an app could take. Introduce permissions even for iOS is, from our point of view, a good thing.

6.2 Android

Regarding Android, we have discovered that the 37% of the applications tested are unsafe. The percentage of unsafe apps is higher than the percentage seen for iOS. However, this study teaches us that the Play Store is not secure. We know that probably without reading permissions we would have found a lower number of unsafe applications. At the same time, through permissions we have had the possibility to understand how much is unsafe the Play Store. Moreover, we have understood that is important to read permissions with the aim to understand beforehand if an app is safe or not. The reader can think now that Play Store is very unsafe or he can think that Play Store is better than App Store because recommends the users on what actions the searched app could do.

As developers, we have noticed that when we want to upload an application on the Play Store, Google publishes our app after two or three hours. So, we think that there is a small control and there is no Google developer that analyzes our application and observes if it does what it has to do. Probably Google has preferred to give a lot of

responsibility to the users that have to understand permissions and the danger they face.

In the upcoming months will be presented the new Android L. The very good news is that, probably, the users will be obliged to accept permissions during the use of the applications [35, 36]. We don't know if it will become something like iOS, where the permissions are shown only when the app needs them, or if it will be a hybrid between Android and iOS. Google has significantly improved its security mechanism based on permissions in this way.

At the same time, we have even bad news for the users. It has been discovered a bug that gives the possibility to unsafe applications to counterfeit some certificates with the aim to have the same privileges of applications like Adobe Flash and Google Wallet [37]. These apps have in fact the possibility to exit from the sandbox (we have discussed about sandboxing mechanism in chapter 1) with the aim to allow specific functionality to other applications. Google Wallet is an application that allows the users to use coupons and credit cards using their devices. So, when you have to buy something on Play Store, on other applications with "In-App purchases" permission or on a website, you can use Google Wallet to pay. This app comes out from its sandbox and comes in the sandbox of the Play Store, of another app or of the browser. So, an unsafe application with this possibility can come in the sandbox of another app, acquire its privileges and read, delete and alter its data. We recommend the users to upgrade the OS of their devices because the bug

is already fixed for Android 4.4 and will be fixed soon even for other versions of the OS. With the new security mechanism based on accepting permissions “at use time”, Android surely improved the security of its operating system. So, Android will be more safe. At the same time, the users cannot forget that there are, anyhow, a lot of unsafe apps and that they can never trust about security mechanisms. Like for iOS, Android users have to document themselves on what’s the purpose of the applications they want to download, they have to be careful on battery consumption, they have to upgrade the OS on their devices and, moreover, they have to read permissions and try to understand when an app is safe or not.

6.3 Summary

In this chapter we have described pros and cons of the respective stores and security mechanisms. iOS, with its applications and its store, seems to be more safe. However, we discovered that there are unsafe applications, backdoors and other problems. Android seems to be more unsafe. We have found many unsafe applications and we have documented a dangerous bug. Anyway, permissions mechanism and the new security mechanism introduced with Android L are positive things.

In the next chapter we will present some conclusions and we will discuss about future works.

Chapter 7

Conclusions

In this thesis we have discussed about the Android and the iOS world. The two systems have some security mechanisms like the memory randomization and the sandboxing mechanism. The two respective stores have their rules and mechanisms to prevent the upload of unsafe applications.

We have seen that the Google Play Store has a great percentage of unsafe applications and that the users can do their best to avoid downloading unsafe apps. We have seen that Apple App Store has a fewer number of unsafe applications, but like for Android we have seen pros and cons. There are a lot of other things to consider. In these years we have often seen a lot of threats for iOS and Android. At the same time, we have seen many changes in regard of security mechanisms.

In these years have been introduced a lot of innovations. For example the notifications when an app tries to use something that undermines the privacy of the user or the stability of the device. However, we have seen that even malware and spyware are increasingly powerful.

We have tested some virtual machines, firewalls, PC and all the tools used with the aim to create the best environment to tackle the analysis phase. Through the analysis we have studied the behaviour of 60 Android applications and 60 iOS applications. The analysis phase has been faced using a network analysis software with the aim to discover principally privacy threats. So, we were very surprised to see that many applications are unsafe. Our idea was to create some statistics and to teach something at the reader. Our purpose wasn't to help the reader understand what system, or environment, or store is better than another. We have conducted this study with the aim to teach the reader how to defend himself from threats.

During the analysis phase we have understood that, regarding Android, permissions are very important for the users. Through permissions the user could understand if he is going to download an unsafe application. However, we have given some tips both for Android and for iOS with the aim to teach the reader how to avoid unsafe apps.

At the end we have thought that even antiviruses could be a quite good solution to avoid unsafe apps. So, we have used some of the well-known antiviruses. We have discovered that there is just one antivirus for iOS and a lot of antiviruses for Android. We have performed the antiviruses test on the Android virtual machine and we have realised that the antiviruses are not very effective. However, they have proved to us that they are capable of identifying some unsafe applications. So, an antivirus on the device can be, anyhow, a small solution for the threats.

We leave the reader with the hope of making him understand that he can never trust of security mechanisms. He is the first that has the task to avoid unsafe applications. As we have seen, unsafe applications and other problems are present in each official store.

7.1 Future Works

The analysis phase that we have shown can be improved increasing the number of applications tested. Our purpose is to continue this study to improve the statistics and to understand if the new operating systems will really increase the power of the security mechanisms.

If there will be the possibility, probably we will create a web platform and an application with the aim to publish all the unsafe and safe apps. More precisely, we want to help the respective stores reporting unsafe apps. At the same time, we want to help the users reporting all the

apps that are safe for the stores criteria, but are privacy threats for our point of view.

This thesis is very useful for people who want to study the same argument in the next months and years. The study can be extended and, at the same time, can be a good comparison to understand if Android and Apple will make steps forward or backward.

7.2 Acknowledgements

I would like to thank my research mentor Gabriele D'Angelo who gave me the possibility to perform this thesis. He has helped me when necessary spending a lot of time. I am very thankful for his patience and for his scrupulous support.

I would like to thank my parents for giving me the opportunity to study, despite the economic situation. Especially, I would like to thank my mother because she has always encouraged me.

I would like to thank all those friends that have always been close to me, persuading me that the university is very important.

Last but not least, I would like to thank my classmates because they have always helped me when necessary.

Bibliography

[1] R.J.G. Vargas, R.G. Huerta, E.A. Anaya, A.F.M. Hernandez. Security Controls for Android. In *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), 2012, pages 212 - 216, IEEE Publisher*.

[2] S. Khan, M. Nauman, A.T. Othman, S. Musa. How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms. In *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012, pages 76 - 81, IEEE Publisher*.

[3] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, C. Glezer. Google Android: A Comprehensive Security Assesment. In *Security & Privacy IEEE, Volume 8, Issue 2, 2010, pages 35 - 44, IEEE Publisher*.

[4] M.S. Ahmad, N.E. Musa, R. Nadarajah, R. Hassan, N.E. Othman. Comparison Between Android and iOS Operating System in Term of Security. In *2013 8th International Conference on Information Technology in Asia (CITA), 2013, pages 1 - 4, IEEE Publisher*.

[5] AppBrain. AppBrain Stats, Number of Android Applications. http://www.appbrain.com/stats/number-of-android-apps

[6] D. Titze, P. Stephanov, J. Schutte. A Configurable and Extensible Security Service Architecture for Smartphones. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2013, pages 1056 - 1062, IEEE Publisher.*

[7] Oliva Hou. A Look at Google Bouncer. *Security Intelligence Blog, July 20, 2012,* http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-google-bouncer/

[8] Sam Costello. How Many Apps are in the iPhone App Store?. *About.com, June 4, 2014,* http://ipod.about.com/od/iphonesoftwareterms/qt/apps-in-app-store.htm

[9] App Store Review Guidelines. *Apple, 2014,* https://developer.apple.com/appstore/resources/approval/guidelines.html

[10] A. Mylonas, S. Dritsas, B. Tsoumas, D. Gritzalis. Smartphone Security Evaluation - The Malware Attack Case. In *2011 Proceedings of the International Conference on Security and Cryptography (SECRYPT), 2011, pages 25 - 36, IEEE Publisher.*

[11] L. Jeter, S. Mishra. Identifying and Quantifying the Android Device Users' Security Risk Exposure. *2013 International Conference on Computing, Networking and Communications (ICNC), 2013, pages 11 - 17, IEEE Publisher*.

[12] Z. Miners. Report: Android malware and spyware apps spike in the Google Play Store - Wallpaper Dragon Ball and Finger Hockey were cited as among the most downloaded malicious apps. *Info World, Security Central, February 19, 2014,* http://www.infoworld.com/d/security/report-android-malware-and-spyware-apps-spike-in-the-google-play-store-236702

[13] Microsoft. Windows FAQ. http://windows.microsoft.com/en-US/windows-vista/Firewall-frequently-asked-questions?498b1000

[14] xNavigation. PC Tools Firewall Plus 7. http://www.xnavigation.net/view/44/pc/tools/firewall/plus/download.html

[15] Wireshark. http://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

[16] Oracle VM VirtualBox. https://www.virtualbox.org

[17] Genymotion. http://www.genymotion.com

[18] E. Blem, J. Menon, K. Sankaralingam. Power Struggles: Revisiting the RISC vs CISC Debate on Contemporary ARM and x86 Architectures. In *2013 IEEE 19th International Symposium on: High Performance Computer Architecture (HPCA2013), 2013, pages 1 - 12, IEEE Publisher*.

[19] BlueStacks. http://www.bluestacks.com

[20] Ubuntu. DoINeedaFirewall, https://help.ubuntu.com/community/DoINeedAFirewall

[21] Wikipedia. Android (operating system). http://en.wikipedia.org/wiki/Android_(operating_system)

[22] C. Marforio, A. Francillon, S. Capkun. Application Collusion Attack on the Permission-Based Security Model and its Implications for Modern Smartphone Systems. *Department of Computer Science, ETH Zurich, Switzerland, pages 1 - 16*.

[23] Wikipedia. International Mobile Station Equipment Identity. http://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

[24] Adobe Flash Player. http://get.adobe.com/it/flashplayer/

[25] Wikipedia. Adobe Flash Player. http://en.wikipedia.org/wiki/Adobe_Flash_Player

[26] Adobe Flash Player exits Android Google Play store. *BBC News Technology, August 15, 2012,* http://www.bbc.com/news/technology-19267140

[27] Z. Benenson, F. Gassmann, L. Reinfelder. Android and iOS Users' Differences concerning Security and Privacy. *2013, pages 817 - 822.*

[28] H. Pieterse, M.S. Olivier. Security Steps for Smartphone Users. *2013, Information Security for South Africa, pages 1 - 6, IEEE Publisher.*

[29] Android Developer, Help. https://support.google.com/googleplay/android-developer/answer/113469?hl=en

[30] Q. Li, G. Clark. Mobile Security: A Look Ahead. *2013, Security and Privacy, IEEE, Volume 11, Issue 1, pages 78 - 81.*

[31] D. Moren. Apple responds to troubling allegation of iOS 'backdoor'. *July 22, 2014, MacWorld,* http://www.macworld.com/article/2456032/apple-responds-to-troubling-allegations-of-ios-backdoor.html

[32] N. Arnold. Is Apple's iOS Backdoor Not a Backdoor?. *July 27, 2014, WallSTCheatSheet,* http://wallstcheatsheet.com/technology/is-apples-ios-backdoor-not-a-backdoor.html/?a=viewall

[33] M. Wood. Apple's Serious Security Issue: Update Your iPhone or iPad Immediately. *February 24, 2014, Bits, The New York Times*. http://bits.blogs.nytimes.com/2014/02/24/apples-serious-security-issue-update-your-iphone-or-ipad-immediately/?_php=true&_type=blogs&_r=0

[34] R. Brandom. The dangers behind Apple's epic security flaw. *February 24, 2014, The Verge*. http://www.theverge.com/2014/2/24/5442576/inside-apples-epic-security-flaw

[35] Exclusive: Android L to Add Granular Permissions Prompt. *June 25, 2014, xdadevelopers*, http://www.xda-developers.com/android/exclusive-android-l-looks-set-to-add-granular-permissions-prompts/

[36] New security system coming with Android L?. *July 28, 2014, Smartphone Virus*, http://www.smartphonevirus.com/news/15-android/18004-new-security-system-coming-with-android-l

[37] J. Forristal. Android Fake ID Vulnerability Lets Malware Impersonate Trusted Applications, Puts All Android Users Since January 2010 At Risk. *July 29, 2014*. *BlueBox*. https://bluebox.com/technical/android-fake-id-vulnerability/