Security with Smartphones

Alicia Sambade Mata

Lusofona University of Porto, Portugal
University of Vigo, Spain

aliciasambade31@gmail.com

Abstract. It is undeniable that nowadays the rise of technologies has caused a big change in our society and economy, and it produces new facilities but, at the same time, problems. Furthermore, the use of the smartphone has become a day-to-day basis and we have more and more functions on them. Despite their success, smartphones have many problems in use and we have to become aware of what dangers we have to face and how to avoid, as far as possible, that they affect us. In this paper, the risks of having a smartphone are going to be analysed and will delve deeper into the security of the Android operating system and some differences with IOS. It will also show some types of cyberattacks and it is going to be analysed from both a theoretical and a practical framework, showing different case studies and showing different solutions and failures in society and technology.

Keywords: smartphones, security, Android, technology, risk, attack, malware

1 Introduction

Nowadays, smartphones have a very important role in our lives, but it is very interesting and surprising how they have evolved to the point where they are now. In 1876, the first telephone communication was achieved and, since then, it has been improved to better adapt to people's lives, until the mobile phone was created almost 100 years later. This point is very important, because since that date many companies have been competing to achieve the best speed in their devices and to be the first to create something innovative. After that, and with the turn of the century, as humans we are looking for more and more comfort and we start to add more and more functionalities to the mobile phone, to the point that nowadays we can do almost everything with it; from basic everyday things like raising the shutter, to work.

Like any change in society, this also has pros and cons. In addition to having faster and real communication, it has become faster to do anything, both to satisfy our needs and for entertainment. New ways of spending our time, new fields of study and new professions that did not exist before have emerged and will continue to do so. On the

other hand, these developments also mean the disappearance of many other jobs, obsolete knowledge and people seeking to take advantage of others because they have more knowledge in this area, leading to the emergence of another type of crime: cybercrime. As more and more people make use of ICTs, the number of people who can be targeted by these attacks is growing, and strong countermeasures must be put in place.

Section 2, *use of smartphones*, describes the current situation of smartphones and the existing operating systems and then focuses on one of them, Android, and analyses it. In addition to a brief comparison with its other strong competitor IOS, its architecture will be explained in section 3. Then, sections 4 and 5 present two case studies that have in common that they are both related to each other by the use of SMS: Joker and Flubot malwares. Finally, methods for securing a device and guidelines on how to deal with malware will be presented.

2 Use of smartphones

Smartphone sales grow exponentially over the years. In the graph below, although we see a decline in 2019, this is due to the COVID-19 pandemic, but even then, it recovers in 2020 and continues in 2021 (see **Fig. 1**).

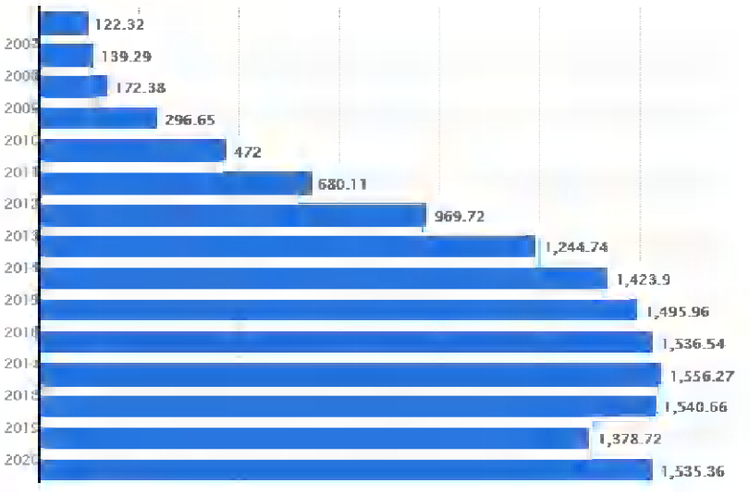

Fig. 1. Number of smartphones sold to end users worldwide from 2007-2021 (million units) [1]

In terms of cybercrime, it is increasing, as is the use of mobile devices. According to a study, the volume of targeted malware threats increases by 15% in 2020 compared to 2019. It was also observed that the threat database grows from 556 million threats in 2019 to around 652 million by the end of 2020, so approximately 17% of these emerged in the last 12 months. It is a reality that there are increasingly better trained specialists to look for vulnerabilities in systems, which we will explain later, and more and more skills are required to combat them [2].

2.1 Security in operating systems

The most representative operating system today is Android, which is the leader in sales (see Fig. 2). The reasons for its success are, among others, the price range of the devices that have it implemented, its wide variety of free applications, the customisation options and the fact that it is open-source software, which allows it to be manipulated for one's own purposes. Despite this, iOS continues to have many Apple brand loyalists and new users and occupies a significant space in the market. Some of the other operating systems available in 2010 have failed to maintain sales in the smartphone area after being beaten by the two giants; in 2017, 98% of smartphones sold had some of the two operating systems (see **Fig. 2**).

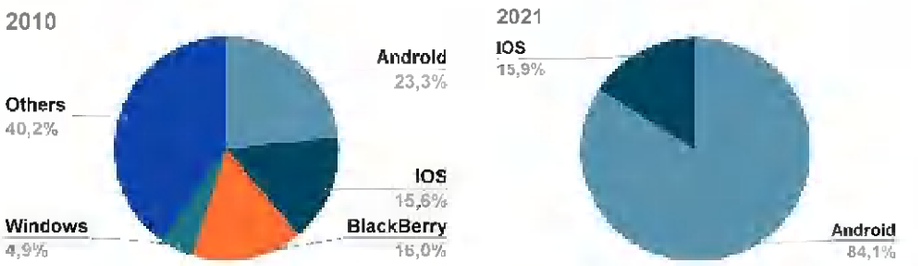

Fig. 2. Global smartphone market share by operating system in 2010 and 2020 [3]

If we make a comparison from a security point of view, the Android model has many different features, but it has certain limitations. Being an open-source software, anyone can access to the source code and test its vulnerabilities countless times. Because of this, it is also very easy to find free apps in Google's shop, Google Play, where there are approximately 3 million apps, while Apple's store, App Store, has approximately 2 million. In addition to the official shop, the Android operating system also allows apps to be installed from external sources in the form of APKs, which carries a risk that does not exist on iOS.

Another characteristic of Android is that it is implemented in smartphones from different companies: Samsung, Sony or Xiaomi, for example. This makes each company's device use software that is not specifically created for it, so some functionalities are programmed with more flexibility and security is more difficult to guarantee. Apple, on the other hand, has strict control over the ecosystem of its devices and how software is deployed, so it has more control over when and how updates are made.

3 Android architecture

Android is an operating system consisting of an open-source software stack based on the Linux kernel and created specifically for mobile devices. This section is important to know how they can be introduced into the system and how they can affect it.

Its architecture is based on 4 layers, depending on the level of abstraction, which form a hierarchy. The first layer is the Linux kernel (the core of the operating system) and is used for abstraction for the hardware, so developers do not have access to it. It provides services to higher layers, such as managing resources (like battery or memory), the file system and allows applications to access it via drivers (be it keyboard, image, audio...). If a manufacturer wants to include some new hardware element, he must create the necessary drivers within the kernel first. [4]

Above this is the abstraction layer (*HAL*). It is made up of several modules, each of which implements interfaces for each hardware component (such as the camera, Bluetooth or the device's sensors).

The next layer is the Android native libraries. Together with the kernel, they form the most important part of the operating system and are programmed in C or C++. Some of the most notable libraries are *libc*, which includes all the headers and functions in C, Media Libraries, which provides the codecs for multimedia content, SQLite, which manages the database or OpenGL/SL and SGL, for the graphics part of Android. [5]

Another section at the same level is Android runtime and includes the Core libraries, which incorporate most of the functionality of the Java programming language, and the Dalvik virtual machine. The latter is a virtual machine adapted to Android's processor and memory limitations, optimising them to the maximum and reducing its execution time.

Between the last two layers is the Application Framework, which includes the classes and services that the applications need in their functionalities, that is to say, the tools for development. Some examples of the APIs it contains are Activity Manager, Window Manager or Resource Manager.

The last layer is the one closest to the user, that of the applications, where you can find native applications (C or C++), managed applications (Java), those that Android has by default and those that the user wants. [6]

4 *Joker* case study

In 2020, Google reported on its blog about the existence of malware that has existed since 2017 called *Joker* hidden in multiple apps on Google Play. It is classified as spyware and belongs to the family called *Bread*. It is one of the most prevalent malware families that continuously infects Android devices and it is not yet certain how many thousands of devices are infected, because more and more apps are being found with this malware, but it has managed to reach approximately 40 countries. What it does is sign the user up for subscription services and trick them into paying these fees. In Denmark, it has managed to sign up thousands of people and earn €7 a week from each of them. [7]

One way to gain access to a device is by using applications that users often use and that are not included on some smartphones. Some of those affected are *Easy PDF Scanner* (to scan a document from a photo), *Now QR Code Scan* (to scan QR codes, bearing in mind that now in COVID time their use has increased), *Super-Click VPN* (to browse with VPN) or *Tangram App Lock* (to lock your items). Attackers need an easy way to access our data, and this is how they get it.

This malware manages to bypass Google Play's app checking mechanism because it continually changes its code and execution methods. On multiple occasions, it gets past Google's filters because when apps are submitted and displayed in the shop they are 'clean' versions and where they installed the malware was in the updates. In this way, the attackers manage to gain the user's trust and permissions for the app and then infect the device.

As a malicious program classified as spyware, it steals information, but specifically the *Bread* family consists of large-scale billing frauds. Early versions were via SMS, but Google has managed to combat them with successive updates; recently, phone fraud is being used. These leverage techniques that involve the user's operator, as they can partner with mobile service providers to allow users to pay for services by SMS. The process involves the user sending a text message with a keyword associated with a prescribed number and then a charge is made to the applicant's bill with their provider. Payment can also be made via the company's website; for this, the user uses his or her phone number and is sent an SMS also with a password Attackers use custom HTML parsers and SMS receivers to automate the process; this is possible because these processes do not require explicit user interaction.

Focusing on a more technical level, *Bread* applications use several methods for string encryption. These include standard encryption, using, within the *'java.util.crypto'* library, encoders such as AES, DES or Blowfish; custom encryption algorithms, using basic XOR or nested XOR; and avoiding basic string matching. In addition, these substrings are sometimes scattered throughout the code and are invoked through static variables or method calls.

5 *Flubot* case study

Another SMS-related case is Flubot, so called because "its spread rate and infection vector resemble the common flu". It is a banking malware and, above all, it is having a big impact in Spain; it is known to have infected more than 60,000 victims and stolen more than 11 million phone numbers. It has been found to have textual content to target German, Polish and English-speaking users, so attacks by this malware are beginning to spread across more territories. [8]

They access the smartphone via SMS messages, supplanting well-known parcel delivery companies such as "Fedex", "DHL" or "Correos", saying that a parcel is about to arrive and that the order can be tracked via the link they provide. Once the user clicks on this link, the malware is installed and searches for an application to overlay

it and obtain the user's credentials, thus also their banking details. Once it has access, it can also make calls, get our contact list and send phishing content or listen to notifications; if the user has linked their phone number to websites of any kind, when user verification is performed, the malware can even get hold of that data.

The problem with this particular malware is getting rid of it. To prevent the user from removing anything from the attacker, the attacker implements mechanisms that stop system protection and the installation of third-party security applications. An Android team has designed an application to safely remove this malware called Malninstall, but many devices are unknowingly infected and will fall victim in the same way.

6 Malware defence and detection

In the present, we can distinguish two profiles of users: the new generations, who grew up in the 'information age', and those who did not. The former, despite having more and better means to deal with possible threats, still do not have a strong understanding of the risks that can come with the use of technology. The latter need to adapt and learn, so they are more at risk of being attacked due to their ignorance on the subject.

On the Internet browsing, attackers can gain access to our data in several ways. One way is to direct the user to a previously infected web page that the user considers trustworthy and obtain all the data entered, or to trick the user into accessing a spoofed page. They also use seemingly inoffensive advertisements, images or any type of file, but with malicious code.

On defence, to begin with, it is essential for a good defence against malware to install all available updates, both to the device and to applications, as they often fix security bugs. As with most devices, one of the most important methods against malware is to install an antivirus. It runs static, dynamic or mixed scans. Static scans focus on observing and investigating the APK, which is defined by AndroidManifest, where the permissions that an application may require, the code with the functionalities (in Java) and the resources it needs, such as database or audio, are declared. Dynamic analysis analyses the behaviour of the system, looking at user interaction or system calls and require excessive resource usage. Mixed analysis is the combination of the two previous ones and is very complete, but it is difficult to maintain due to the cost of development and maintenance [9].

The antivirus requests a lot of permissions from the device in order to scan all data for compromise and it is very important to get it from a trusted site, because many attackers can hide malware in such applications. In some cases, fake advertisements are used, warning that the device may be compromised and prompting people to download an antivirus, which most of the time is free and contains malware. Although

this is important, it is not essential, because by surfing safely and being cautious, an attack can be avoided.

As mentioned above, it is very easy to install third-party applications on Android due to its freedom at the operating system level. For apps in the Google Play shop, there is a review by Google Bouncer that looks for malicious software and compares it with other apps to identify malware and remove the app, if applicable. Apps that are not on Google Play lack this review, so be careful when downloading them. A good way is to do it from APK repositories that use filters and are secure; it is very important to know the origin of an APK when you intend to use it. Remember to have the *Install apps from unknown sources* option deactivated and, in any case, activate it only when necessary.

Regardless of how you obtain the application, you should always carefully examine the permissions that are requested before accepting them, as some may be unnecessary and indicative of suspicious activity. Currently, many of them have the option to activate them only when the application is in use and it is a good method to control access to data or functionalities and make use of them when they are not required; it is a method to protect yourself but also to control resources. It is recommended to review and update from time-to-time what permissions are granted to each application in case there are any suspicious or unneeded ones. This can be done from the device's settings. In the image, we can see the permissions given and denied to a video playback application; none are accepted because they are not necessary (see **Fig 3**).

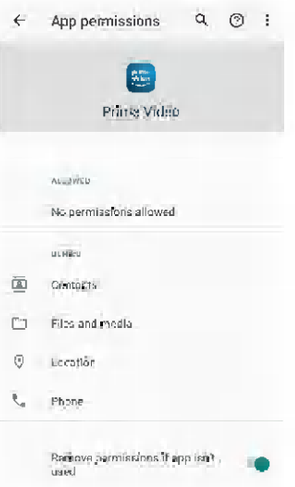

Fig. 3. Application permissions in *Device settings*

The appearance of excessive advertisements or in non-advertising applications and unknown installed software are signs that malicious activity may be occurring. Battery or data usage can also help to detect this, as excessive or unidentified data usage

can mean unknowingly running functions in the background. Android warns if it registers anomalous activity, identifies it and allows an action to be taken (see **Fig. 4**).

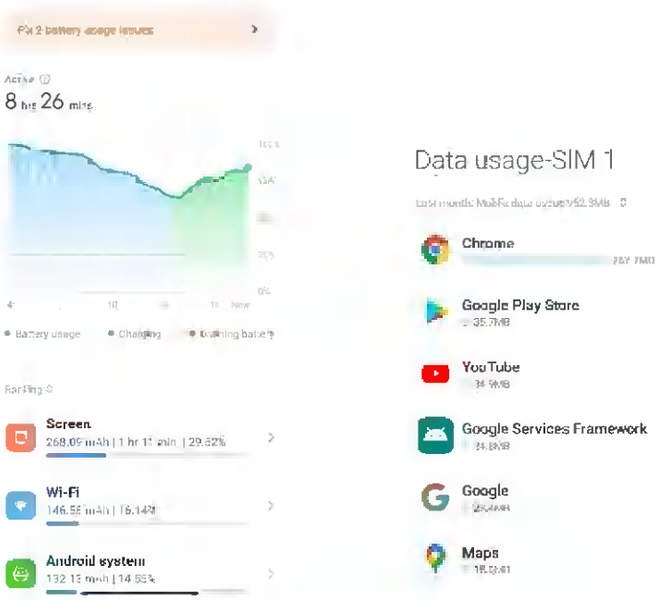

Fig. 4. Battery and mobile data usage in *Device settings*

In **Fig. 4**, the user charges the phone before reaching 50%, so it is not possible to see the full waste that the battery would have. However, it is still possible to see how much the screen and Wi-Fi consume; even if you are not aware of the consumption in *mAh (Milliamp-Hours)*, you can see the percentage and reflect on whether this consumption has occurred (if the screen has been on for a long time or if the Wi-Fi has been activated). Many malwares may have made use of these and other resources, and the user may not have perceived it; is convenient to observe and analyse it. The same happens with mobile data usage; it is normal for video or gaming apps, for example, to have a higher consumption. If we have identified a big change in applications that do not require internet or an unknown application, we need to take action.

In Dual Sim smartphones, such as the one shown in **Fig. 4**, the usage of the other card (SIM 2, in this case), which is not used as the main card for mobile data usage, should also be observed, as unknown or excessive usage may have occurred in the background.

6.1 Remove malware

Even if you take precautions, you can still fall victim, because now there are multiple ways for malware to enter a device without leaving traces. If you see signs that your

device may be infected, it is best to perform a factory reset because you don't know the extent of the attack and what it does. This can be done from the console that can be accessed in the phone's power-on process or from the phone's settings. The result of this is that all data except system and manufacturer applications are deleted; the /data, /sdcard and /cache partitions are deleted.

Before this, if you do not want to lose the information on the device, you can make a backup, but to do this you must switch the smartphone on in *Safe Mode* (see **Fig. 5**). This mode starts the system only with the system and manufacturer's applications and does not run third-party applications. In this way, we can safely back up our data and, if we have identified the malware-causing application, uninstall it.

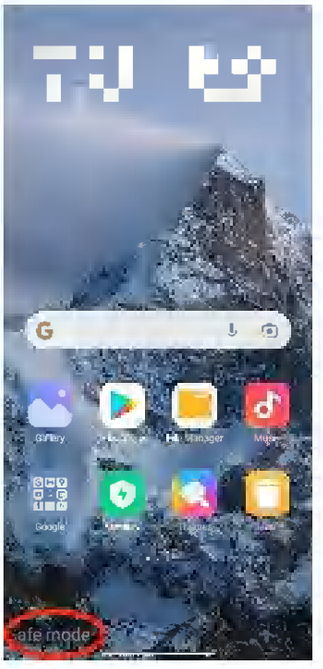

Fig. 5. Smartphone started in *Safe Mode*

7 Conclusion

Many changes have occurred in society with the existence of technology, but they will continue to happen, and people must adapt to them. It is essential that people are taught about all that technology brings with it, both the good and the bad; people need to know how to protect themselves from these possible attacks or, at the least, to avoid great harm. The smartphone has become, for many people, another part of the body with which they can carry out most daily actions and which has all their data; moreover, people are not aware of the information we have inside a mobile phone,

both our own and that of those around us. There are cases like Joker, Flubot or many others with important consequences, so worrying about the security of a device has to become a regular routine in our lives; browsing safely, checking permissions given to apps and being aware of any suspicious activity are small actions that can avoid big problems.

References

1. Cell phone sales worldwide 2007-2021. Published by S. O'Dea, Dec 16, 2021
   URL: https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/
2. 2020 Threat Summary by Alexander VukcevicAvira Operations GmbH, part of NortonLifeLock Inc. (2021)
   URL: https://www.avira.com/en/blog/2020-threat-summary
3. Gartner Says Worldwide Sales of Smartphones Grew 9 Percent in First Quarter of 2017, Gartner, Inc. (2017)
   URL: https://www.gartner.com/en/newsroom/press-releases/2017-05-23-gartner-says-worldwide-sales-of-smartphones-grew-9-percent-in-first-quarter-of-2017
4. Vanegas, C. A. (2012). Desarrollo de aplicaciones sobre Android. Revista vínculos, 9(2), 129-145. [Spanish]
   URL: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/4275/5967
5. Puente Arribas, D., Daguerre Garrido, J. I., & Costales de Ledesma, R. (2021). Malware Analysis on Android. [Spanish]
   URL: https://eprints.ucm.es/id/eprint/66842/1/COSTALES%20DE%20LEDESMA%2064210_RAMON_COSTALES_DE_LEDESMA_Malware_Analysis_on_Android_784051_190326 1751.pdf
6. Programming on portable mobile devices [Spanish]
   URL: https://sites.google.com/site/sweuc3m/home/android/generalidades/2-2-arquitectura-de-android
7. PHA Family Highlights: Bread (and Friends) (2020)
   URL: https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html
8. FluBot - Malware Analysis Report (2021)
   URL: https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf
9. Heras Cáceres, I., & Sierra Liras, D. (2015). Sistema de detección de malware en Android. [Spanish]
   URL: https://eprints.ucm.es/id/eprint/33026/1/memoria_TFG.pdf