Department of Computer Science

Master Seminar

Security of Mobile Devices

Submitted at:

09. July 2019

Author:
Lukas Janssen

Supervised by:
Prof. Dr. Gerd Beuster
Fachhochschule Wedel
Feldstraße 143
22880 Wedel
Phone: (041 03) 80 48-38
E-mail: gb@fh-wedel.de

Contents

1 Introduction

In the last years the amount of mobile devices grow explosive[1] and for this trend is no end in sight. Meanwhile, these devices are more connected than ever before and the connectivity has a higher coverage worldwide with faster speed. Often mobile devices contain sensitive data of the user or a company, which can be an interesting target for an attacker. More targets on mobile devices are discussed in Chapter 2.

Today, the most common mobile device is a mobile phone. Over 3 billion people on the world use a mobile phone[2]. Other common known mobile devices are tablets or laptops, but today the types of mobile devices are much larger. Smart watches become more and more popular and our modern cars are connected, too. Many other devices exist around the world, for example there exists smart devices to measure the air quality, that you can take with you. Most of thes devices can connect everywhere to the internet via cellular infrastructure. Approximate 63% of world population have internet access through a mobile phone, see figure 1.1.[3]

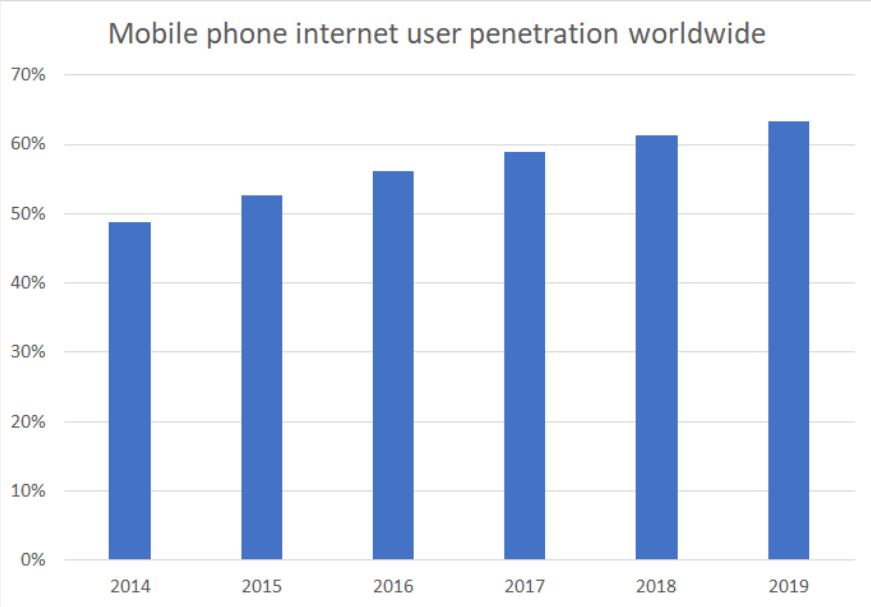

Figure 1.1: Percentage of the global mobile phone population accessed the internet from their mobile phone.

Erricsons says, that around 95% of the world population can have access to mobile internet over a cellular infrastructure. In 2016, 55% of the world population can have access to fast LTE infrastructure. Erricson say also, that in 2022 the coverage of the LTE infrastructure grows up to

80% of the world population. 5G coverage will begin in metro regions and archive 15% coverage until 2022. LTE is growing much faster than HSPA, only 5 years instead of 8 years to archive 2.5 billion peoples.[4]

The market for mobile phone operating systems is dominated from two providers, the first is Apple with the iOS system and the second is Google with the Android system. Android is the most used mobile operating system worldwide, it runs on 88% of all mobile phone worldwide.[5] The iOS mobile operating system is installed only on approximate 11% of all mobile phones. It is only distributed by Apple itself, Android instead are distributed by many manufactures like Samsung, LG, Huawai, Google itself and many more. But Android has a large problem with version fragmentation, because of this large amount of manufactures. This will be discussed in Chapter 3.2. In comparison to IOS, Android has fifty times more malware infections, details of this will presented in Chapter 3.1. Mobile devices can be infected in different ways[6]. One way is to load an app in the app store with malicious code. An Android app can also be installed by side loading, this means that the app will be installed directly, without a app store. These side loaded app will not be scanned by the app store provider for malware and will be less secure. Another way to infect a mobile device with some malware are websites, where the user automatically downloads malware, if he visits the site. Direct attacks on a device are also possible, especially because the mobile device will travel through different networks and can be connected to the same Wi-Fi, like the attacker. Or the attacker has direct physical access to a device and is able to place some malware on it.

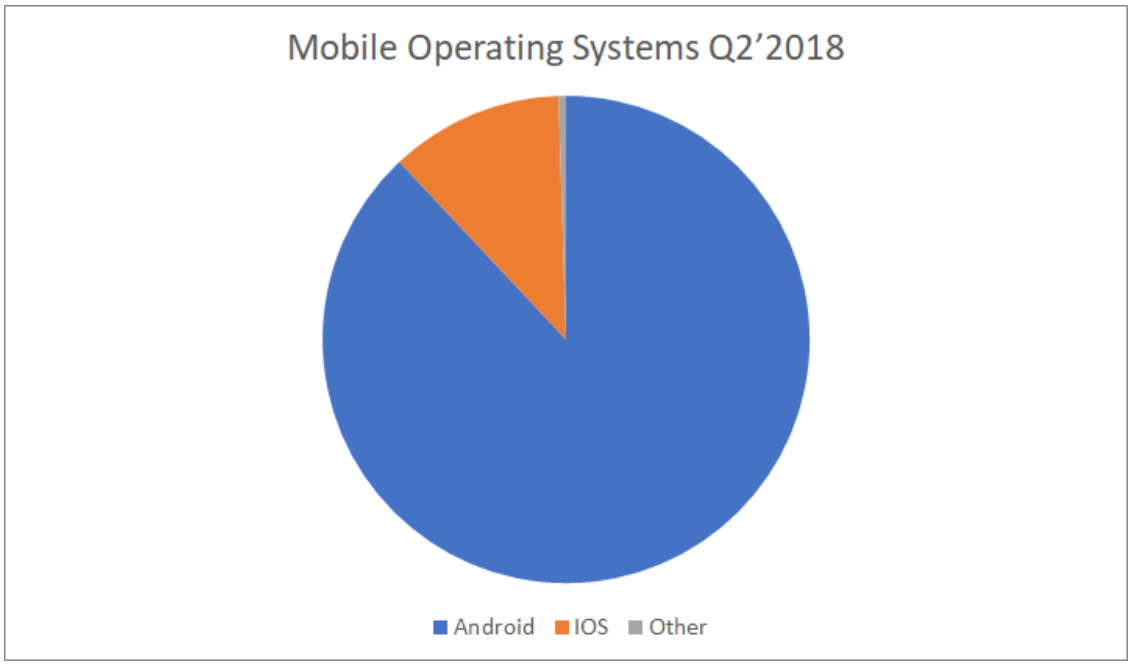

Figure 1.2: Percentage of different mobile operating systems of the entire market in the months april to june 2018.[5]

In this paper we will discuss different targets of mobile devices and some security problems, that exists in context of mobile devices.

2

Targets on mobile devices

2.1 Steal sensitive data

Mobile devices and especially on a mobile phone store sensitive data, which can be an interesting target for an attacker [7]. If an attacker got access to a mobile device, he can steal this kind of information and e.g. sell it on a black market or do other criminal activities with this information.

This data can be personal identifiable information, which the user have saved on the mobile phone. This can be virtual information like usernames, email or passwords, but also information of the real world, like the full name, birthday or address. This information can be used to impersonate someone else. Moreover, the address book of a mobile phone stores over all contacts of the owner. This includes the name, contact information and sometimes ever bank information of other persons. Additionally, mobile phone store message logs, about when the owner communicate with his contacts. This gives a lot of information about the owner and can contain a lot of secret information. Some secret information frequently stored on a mobile phone are the financial data of the owner. These are often used to buy some app or buy stuff in an online market. This information can be stolen and misused by the attacker. Last but not least, most mobile devices store information on the owner himself, like a movement profile, where the GPS coordinates of the user are saved. The mobile device also store health information from different sensors like a heart rate sensor. This information indicates the health of the owner.

A mobile phone is also always equipped with microphones, a camera or other sensors which may used by an attacker to get additional information about the environment. This can be used to attack the victim in the real world, see Chapter 2.5.

2.2 Steal company secrets

More and more companies give their employees a smart phone for working purposes. So these devices will be used by the employee to call customer or coworkers, write and receive mails and additional they will view and sometime edit documents of the company. These activities result in a large amount of company data with a lot of company secrets on the device. These secrets can be a target for an attacker. These devices move through non-company controlled networks (public Wi-Fi's or cellular infrastructure), not like tower computer within the company network. So these

devices cannot be shielded against direct attacks. Same applies to company notebooks with the employee privilege of home office.

Another thing that companies today often allow is “Bring your own device”, this means that an employee is allowed to use his private devices in a company context. So the employee is able to do work related activities on his private device. As a result of this, company data are stored and accessible from a non-company controlled device. This increase the security risk, because the company cannot fully control the device. Some company have restriction on devices and settings that are allowed as “Bring your own device”. For example, the device must be always up-to-date, to reduce exploits for the device. Some other rule for the device setting can be, that a accurate authorization is enabled and enforced on the device, like a password with enough characters, two factor authorization or biometric authorization.

2.3 Monetization through premium SMS and calls

Most mobile phone contain a SIM card from a provider, which the mobile phone can use to connect to the cellular infrastructure of this provider. With this SIM cards the provider can track the activities like call someone or send SMS’s. Base on this data, the provider will bill the customer. These services can also be used to pay third party services, like premium-rate numbers or hotlines. Same for third party contracts, you can pay over your mobile phone contract. This can be used by an attacker, if he gets access to the mobile phone, he can send SMS’s to such third party and generate cost for the owner of the mobile phone, while the attacker enrich itself with the service. Mobile providers offer to block this kinds third party costs, this will decrease the risk from this expensive invoices from this side. If the attacker is able to send messages to some third party and create some cost for the owner of the mobile phone, he will intercept incoming SMS to block the billing information. So the user will not be notified over the billings and the whole attack will run in the background. Furthermore, the attacker can use text messages to distribute malware to other mobile phones, for this the attacker can use the contacts phone numbers in the address book on the mobile phone.

2.4 Bypass 2 factor in authentication

To improve authentication of some services, the use of a second factor (beside the traditional username and password combination) for authentication becomes more frequent. This second factor can be “something you have”, like a hardware token. Another “something you have” factor can be an authenticator app or a message, received by email or SMS. All these factors can be implemented by a mobile phone. This mean, that often the mobile phone is used as a second factor. In the last years, 2FA via mobile phones increased, see figure 2.1 to see the trend in the united states. The problem with 2FA over a mobile phone is, when an attacker is able to access to the mobile phone, he is able to take the second factor of some service, too. So the second factor will not increase the

security in authentication, because the factor, that you and only you have something, will not hold once the attacker has access.

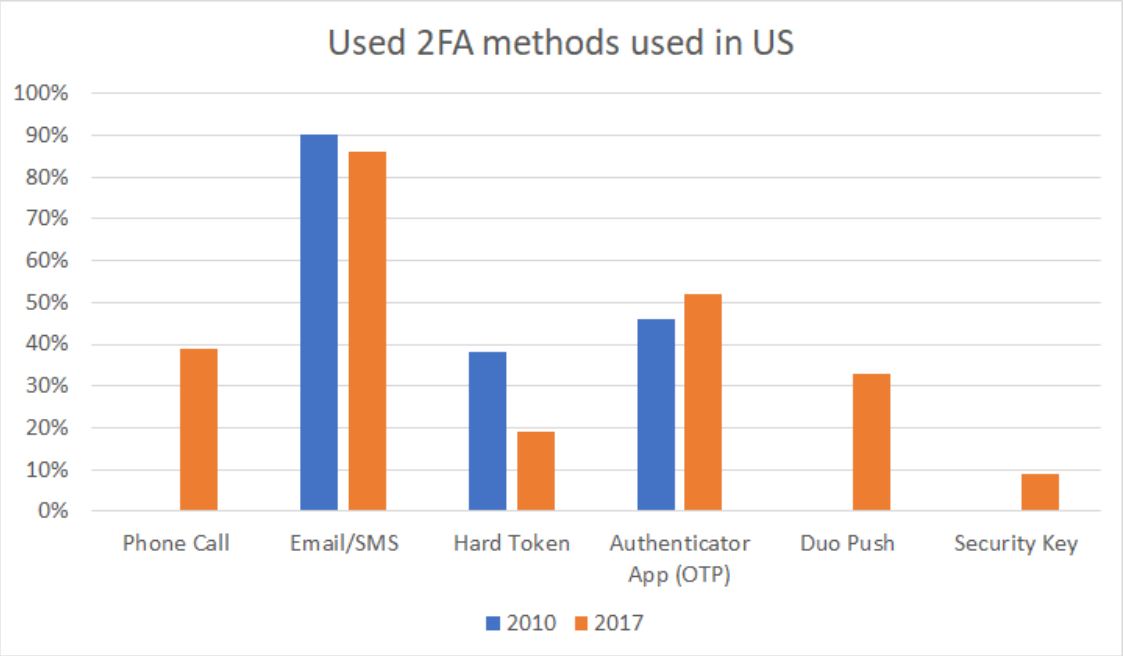

Figure 2.1: Percentage of methods for two factor authentication method used in the united states 2010 vs 2017

2.5 Attack person in real world

Mobile devices will be most time near the owner, especially mobile phone are in the modern world everywhere. If an attacker get access to the device, he is able to read all kinds of sensors of the device. These sensors will give the attacker a lot of information about the owner's geo position or the current activities of the owner. This can enable traditional crimes like burglary, kidnapping, stalking or in extreme cases terrorist attacks. The attacker can time a burglary to the house of a person, if he is not at home, because he can track the position of the owner by his mobile phone. Alternatively, he can kidnap or stalk the owner, because he knows, the position of the owner. Additionally, he can stalk the owner full digital, because he can receive data of the sensors, like the camera over the internet and stalk the activities of the owner by this information.

Another attack is manipulate the phone, so the user cannot call emergency numbers. In an emergency cases the person will not be able to call emergency, this can result that some person die or the police will not reach a crime scene, because they cannot be notified.

A second way to manipulate a person in real world is to manipulate life-affecting devices like NFC-based insulin pumps. If this will not work correct, it can be very dangerous for the victim. The same holds for other connected devices, which can produce a large impact in the real world, like a car. If an attacker is able to access the control logic of the car, he can drive the car via remote connection when he wants. This depends on the car model, if this is technically possible.

3

Current situation

3.1 Mobile malware phenomenon

The mobile malware phenomenon started a couple years ago, where the amount of mobile malware grow explosively. This happend because the development of mobile malware changed from development for fun to development for financial profit. The rate of mobile malware was in the last years very high, but the last peak of mobile malware was at begin of 2017 [8], with a monthly infection rate of 1,3%, after this peak, the amount shrank a lot. This has two different reason, first, the mobile operating system increasing their security a lot, resulting in more secure mobile devices. Most malware is downloaded from app from the normal app stores, but this stores increase their security checks in the last years. Furthermore, cybercriminals currently focus more on IoT devices, than on mobile devices, because the amount of IoT devices grow fast and they are often less secure and easier to attack, than a modern mobile device. This does not mean, that mobile devices are not longer a target for an attacker, the amount of mobile device malware still grows. Nokia has at beginning 2019 near 20 million Android malware samples in their database, in the year 2017, they only had around 10 million samples. The most detected Android malware in 2018 was Android.Adware.AdultsSwine, which is an adware, that display inappropriate ads from the web, like pornographic ads with the target to trick the victim to install fake security apps to remove these ads [8]. This fake security apps shows ads, too. And these ads can only disabled by registering for premium services with hidden costs.

As already mentioned in the introduction, the Android system is more vulnerable for mobile malware. In numbers, fifty times more malware infections on Android than on iOS. The main reason for this are the ability for side loading of apps [8]. Because if this is once enabled, the apps can be installed from everywhere. This mean, an attacker can manipulate the files of a common app with some malicious code and upload it to a file share. After that, the attacker can use phishing, advertising or other social engineering technics to route a victim to his app and install successful the malware on the mobile device of the victim. iOS apps are basically limited to a single source, the Apple Store itself, fully controlled by Apple. This mean every app will be scanned by Apple, before it ever installed on a iPhone.

3.2 Update problem on Android

In the Android ecosystem exist many manufactures for mobile devices. The base operating system is developed by Google, but most manufactures like Samsung, LG or Huawai will customize the system. At least to optimize the system for the own hardware and create a customized skin. If a new version is been release by Google, the manufactures need to modify this updates, before it can be roledout to the customer. These changes will cost the manufacturer a lot of money, if they want to support devices over many years. Therefore, the manufacturer does not support many feature update for their devices. Most Android devices receive software updates only two years after release, mostly this are one large feature update[9]. Apple instead updates their devices for five years after release. Because of this, many different Android versions and often old version running in the world, see figure 3.1[10]. This is a statistic by Google, where they measure all active Android devices in a seven day period at beginning of May 2019. Google itself has dropped the support for Android 6.0 and below. Thereby over 42% of all running Android systems are no longer supported and will not receive any security update and the manufacturer don't want to update to a newer Android version. This issue with non up-to-date versions of Android devices will increase, consider the situation in regard to security patches. Most manufacturers skip some security updates or roll them out significant delayed. In numbers, Android releases every month a new security patch and these will be instant rolled out to Google's own Pixel phones. But other Android phone like LG G6 get security update only three times per year. This means, that most Android devices, which are currently in use, are not able to be up-to-date and have known security issues.

3.2.1 Project Treble

A solution from Google to solve these update problem of Android is Project Treble. The target of this project is to make the Android system more modular[11]. This mean, that the manufacturers custom implementation can be used over different Android versions, without refactoring. With Android 8.0 Google add a stable vendor interface for hardware access. This hardware abstraction layer (HAL) enables Android to be independent of low-level device driver implementations[12]. HAL implementations are packed into modules like camera, sensors or storage and the Android system can load these modules at proper time. This HAL modules will be defined by HAL interface defined language and stored at a special vendor partition on the storage. If all customization for the hardware will be defined in this partition, the Android system is able to be replaced, without rebuilding the HAL's. In previous versions of Android, most manufacturers make customizations direct in the Android code base, and an update was a huge effort. This new modular system make the development process of manufacturers faster and cheaper, if a new Android version is released.

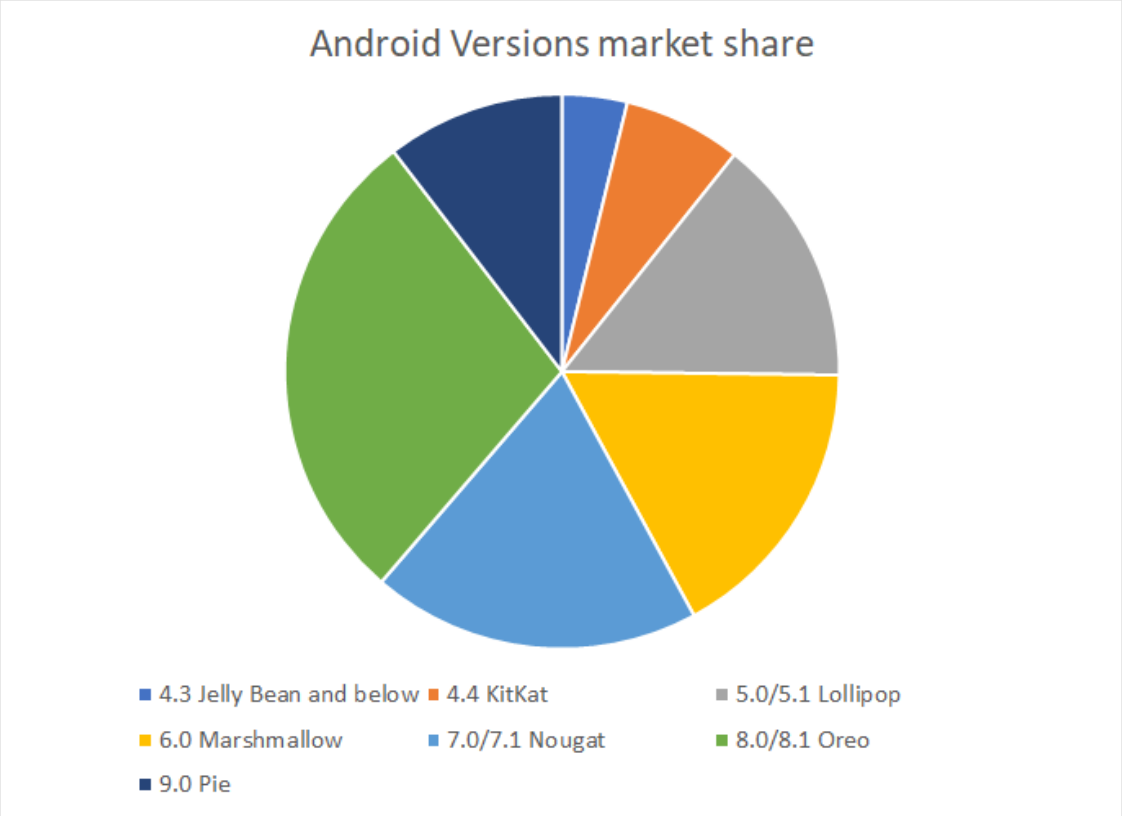

Figure 3.1: Percentage of market share of different Android versions.

3.3 Frameworks for analysis

To analyze if a mobile device application is malicious, there exist many different frameworks. Some of these, analyze the apps dynamic runtime behavior and other run a static analyze to check all execution paths. But first must be defined, what is a malicious action from an app. Is sending an SMS in background, really a malicious action? Or receive data from external sensors like GPS and sending this data via network to a server? What actions are really malicious? This is difficult to say, because sometime these actions are required for the normal function of an app. Like sending the current position to a map app provider. Therefore, current research and analysis frameworks try to understand, analyze and mitigating malware threats. Some example of Android analyze frameworks will be shown in the following [1].

DroidScope is a framework with dynamic approach, in practice, this mean that DroidScope used the Android emulator to run the Android system virtual. In this virtual environment DroidScope deploys a virtual machine to gather information about the system, on the OS-level. Additionally, DroidScope exposes hooks for Android's API's. This allows to run fine and coarse-grained analyses, like tracing system calls, single instruction tracing or taint tracking. The problem with this approach is, that DroidScope does not run analysis on its own, it only supplies tools, which can be used to run analysis.

TaintDroid is also a framework with a dynamic approach. The main goal of this framework is to identify data leakage of sensitive information. Therefore, it tracks information flows between the system and application and between two different applications. These flows can proceed over different ways in the complex Android system. So TraintDroid offers instrumentation on different levels for analysis. TraintDroid shows information on information flows by native methods or interprocess communication(IPC). It is able to show this information by patching the Java Native Interface(JNI) call bridges and the IPC binder library. The problem with this is, that this technics modifies the internal Android component and this can be detected by malware.

DroidBox is an in-the-box Android malware analyzer, that is build on top of TraintDroid. It uses also custom instrumentation of the Android system and kernel to track behaviors. Because of these two tracking methods, DroidBox can be easily detected by malware and the malware can circumvent the tracking or worse, disable the tracking and the malware will be hidden from DroidBox.

Andrubis is like DroidBox an in-the-box Android malware analyzer, which is basically based on TraintDroid and DroidBox. For this reason, Andrubis shares the weaknesses of both. It can also be easily detected by the malware.

CopperDroid does in difference to the others an automatic out-of-the-box dynamic analysis[13]. Therefore, CopperDroid uses a unified system call-centric analysis to specified behaviors in low-level OS and high-level Android. This includes also IPC and remote process call(RPC). Based on the observation that all behaviors will eventually invoke a system call, this information should be enough to identify malicious action. CopperDroid was very effective to successfully disclose additional behavior in a test with over 1300 samples of malware.

Google Bouncer is the official scanner for malicious application of the Google Play store. It is named bouncer, because if a developer wants to upload an application, bouncer will check the application for malicious code and bounces the application in case of successful detection. More information about the exact method to check uploaded apps is not available. Only that it is also a dynamic analysis framework based on virtual Android environments.

SmartDroid use a hybrid analysis, with static code analysis to identify paths to suspicious actions and dynamic analysis to determine UI elements which will execute the path that are identified by the static analysis. For this analysis, SmartDroid use both, an Android emulator and Android internal component to identify the UI elements. The problem is that SmartDroid is vulnerable for obfuscation and reflection, because this make it very hard to statically determine all possible execution paths.

4

Conclusion

Security of mobile devices is an important issue. Mobile devices are everywhere, the numbers are growing, and they travel through different foreign networks. Therefore, the devices need to be secure. Additionally, a mobile device often have access to much personal information like personal identifiable information or sensor data of the device itself. If this data can be access by a wrong person, it can be very dangerous. The security of these devices has increased over the last years, but the security still be an issue. The security of the Android system will increase continuous by different malware analysis frameworks. But the large Android problem of version fragmentation still exists.

Bibliography

[1] E. Markatos, D. Balzarotti, M. Almgren, E. Athanasopoulos, H. Bos, L. Cavallaro, S. Ioannidis, M. Lindorfer, F. Maggi, Z. Minchev, *et al.*, "The red book," 2013.

[2] D. Neitzke, "Themenseite: Smartphones." https://de.statista.com/themen/581/smartphones/. visited on 22.06.2019.

[3] "Global mobile phone internet user penetration 2019 | statistic." https://www.statista.com/statistics/284202/mobile-phone-internet-user-penetration-worldwide/. visited on 15.06.2019.

[4] "5g global population coverage – ericsson mobility report." https://www.ericsson.com/en/mobility-report/population-coverage, Nov 2018. visited on 15.06.2019.

[5] "Mobile os market share 2018." https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/. visited on 15.06.2019.

[6] "4 ways hackers are infiltrating phones with malware on android phones." https://www.wandera.com/mobile-security/mobile-malware/malware-on-android/. visited on 22.06.2019.

[7] E. Anthi and G. Theodorakopoulos, "Sensitive data in smartphone applications: Where does it go? can it be intercepted?," in *International Conference on Security and Privacy in Communication Systems*, pp. 301–319, Springer, 2017. visited on 15.06.2019.

[8] "Nokia threat intelligence report – 2019," *Network Security*, vol. 2018, 2018. visited on 15.06.2019.

[9] "Only two android brands score reasonably well in analysis of security updates - 9to5google." https://9to5google.com/2018/02/28/android-security-by-brand/. visited on 22.06.2019.

[10] "Distribution dashboard | android developers." https://developer.android.com/about/dashboards. visited on 15.06.2019.

[11] "Here comes treble: A modular base for android." https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html, May 2017. visited on 28.08.2019.

[12] "Android architecture: Android open source project." https://source.android.com/devices/architecture. visited on 28.08.2019.

[13] K. Tam, S. J. Khan, A. Fattori, and L. Cavallaro, "Copperdroid: Automatic reconstruction of android malware behaviors.," in *Ndss*, 2015.