Android - Security Metrics
-Draft-

Alexandru Babeanu 4881133
Antoine d'Estalenx 5149371
Irène Förstel 5149398
Arjen Brussen 4974484

September 16, 2019

1 Introduction

Android is an operating system developed by Google to be used for mobile devices. First released in 2008, it has become the dominant operating system for such devices, with a market share of 84% (Fig. 1). Its large user-base makes this operating system a very appealing target for threat agents, since the more victims are impacted by an incident, the more revenue is generated for the attacker. Figure 3 shows the most common types of malware that target mobile devices. The most common malicious activities that target mobile devices include:

- The theft of personal information thorough spyware applications. This data may involve address details, location data, bank account information, etc.
- Performing unauthorized calls or messaging to increase the revenue of specific services at the expense of the victim.
- Presenting unwanted advertisement to users via adware.
- The theft of computational resources by cryptocurrency miners.

The programs that run on these devices, called "applications", or "apps" for short, offer various attack vectors for threat agents, such as exploiting vulnerabilities found in existing legitimate applications, or intentionally publishing applications with vulnerabilities or malicious behaviour. These programs are offered by a large number of vendors and distributed through public online marketplaces called "app stores". Most Android applications are distributed through Google Play (Fig. 2), an app store run by Google, but many other app stores exist. Each store has its own set of rules and requirements regarding the software that can be published on them, with varying attitudes towards security and privacy, and with different moderation capabilities.

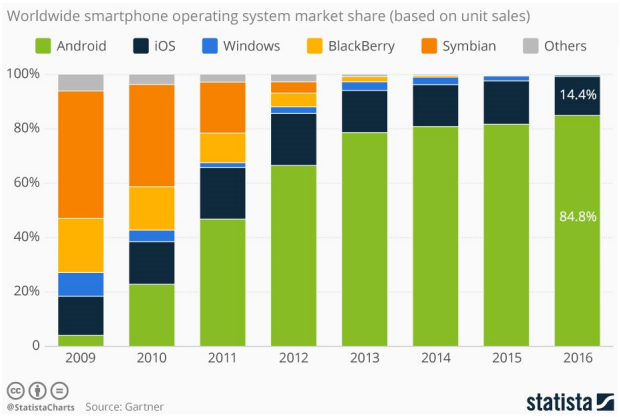


Figure 1: Worldwide smartphone operating system market share (based on unit sales), source: [6]

This brings into question how trustworthy some of these app stores are, and introduces the need for a method of evaluating how safe the products published on these stores are. In paper [3], the authors perform a security comparison between various app stores, considering the controls they have in place and how efficient they are at combating malware. In some of the stores considered for this study, the percentage of apps that were detected to contain or be malware was over 50%. This showcases the importance of evaluating these markets for the safety of their users.

2 Methodology

Note: we are slightly unsure on what to put here, as it was not clarified well in the assignment instructions or in the submission instructions. If possible, could you advise us on this at the upcoming meeting?

Using the information provided, we can estimate the security level using (some of) the four metrics we have learned in block 2. Based on existing literature, we could find out which metrics are the most practical for making security decisions. Then, we can provide an analysis on the platform level as well on general application level (security in application themselves is also an issue). Lastly, we could evaluate these metrics on the data that was given to us and come to a conclusion on the practicality of these metrics.

3 What security issue does the data speak to?

The data can be described as a list of applications with some information about them: The category an application belongs to and the amount of downloads per category. Furthermore, results of analyses of the apps by various

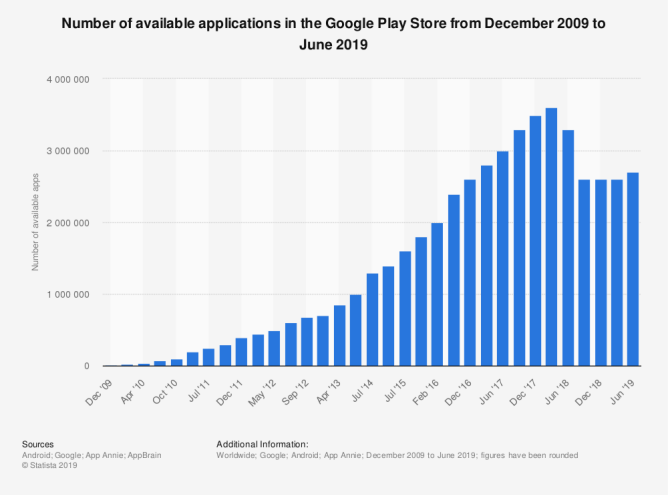


Figure 2: Number of available applications in the Google Play store from December 2009 to June 2019, source: [7]

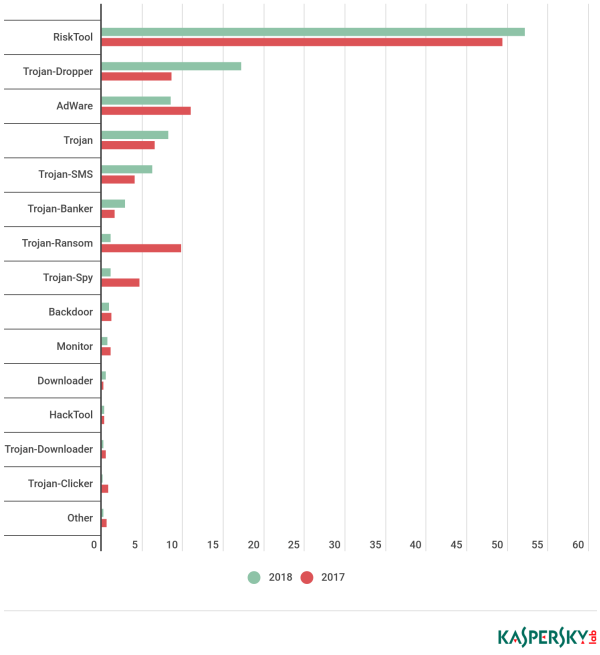


Figure 3: Distribution of new mobile threats by type (2017 and 2018), source: [8]

antivirus software **(insert antivirus names and analysis results)** are given, presenting us with the ratio of infected apps per category. Therefore, the security issue at hand is the amount of malware in multiple application stores easily available by end-users. Most of these applications come from an .apk file. These files are often found on non-verified stores since the Google Play Store does not give immediate access to apks. Therefore, most .apk files were uploaded without having to pass integrated security checks (such as the Google Play Store). These files come from the following datasets which correspond to the respective online application stores:

- eoemarket.com
- freewarelovers.com
- gp09, which is probably apkmonk now
- liqucn.com
- mumayi.com
- playdrone, which analyses applications from the Google Play store

Issues : Are there substantially more malware-infected apps on non-verified stores than on the Google Play store? Is the Google Play store more secure since it is the official store?

Another security issue that could be addressed with the data is the quality of mobile antivirus software: are they efficient? Can they detect every malware? Is there a lot of false positive or false negatives?

Lastly, we could also analyze the security level of applications. So far we only talked about platform analysis, but the code quality of applications themselves may present many vulnerabilities not caught by any of the utilized antivirus applications.

4 What would be the ideal metrics for security decision makers ?

In order to measure the security of the Android world, we need some metrics. Ideal metrics would be huge data from the stores. For example, having the total number of daily downloaded applications and the total amount of malware downloaded per day could allow us to have a representation in time of the number of infections, and give us an overview of the quality of the controls in the stores (to check whether an app is malicious or not), even if it also depends on the behaviour of the attacker. We could also measure the number of malicious applications per application type (whether it's a game, a fitness app, a messaging app...) to understand which types are targeted and why (because they have better controls ? or because one type of application leaks more information than

the others ? For example fitness and running applications can leak the location of the user, which is useful for burglars).

Possible metrics :

- Amount of downloaded malware (normalized per day)
- Identify malicious publishers and developers ?
- Measure the quality of available antivirus software ?

To assess the quality of antiviruses one could count the number of false positive, false negative... But it is not that easy : how to find those values ? How to check if an app is really a malware ? One could also check if the quality of antiviruses related to their budget / price ?

Possible metric : If an antivirus detects a virus, how many others do ?

5 What are the metrics that exist in practice ?

Metrics about security flaws in existing software/apps (not about malwares apps) Malwares are detected through resource consumption [4] or by tracing system calls [5].

6 A definition of the metrics that can be designed from the dataset

We can count the number of applications depending on the category and count the number of malwares in each category : we can then have a first idea of the targeted applications and the targeted customers. That would be one metric that informs us about the threat environment of the Android ecosystem for a user

This can be linked with the popularity of the categories, which can be measured by summing up the number of downloads in each category :

Another metric would be the reliability of the anti-viruses : some anti-viruses never detect the threats, they show a poor quality of controls.

7 An evaluation of the the defined metrics

8 Conclusion

References

[1] Paul E. Black, Karen Scarfone and Murugiah Souppaya: "Cyber Security Metrics and Measures". In Wiley Handbook of Science and Technology for Homeland Security, 2008.

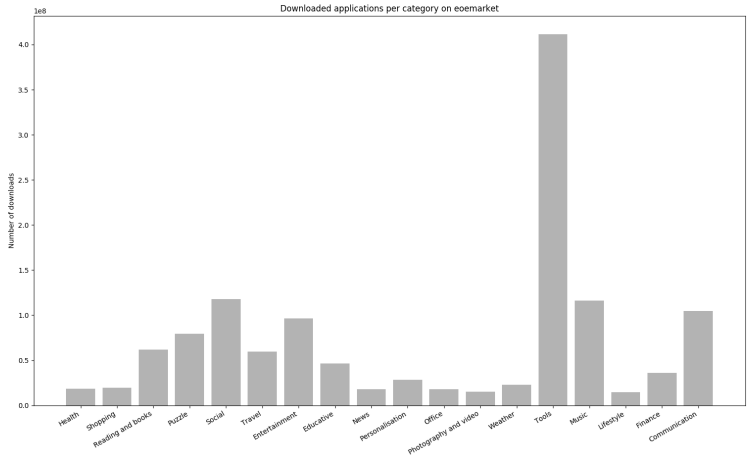


Figure 4: Infected applications per category on eoemarket.com

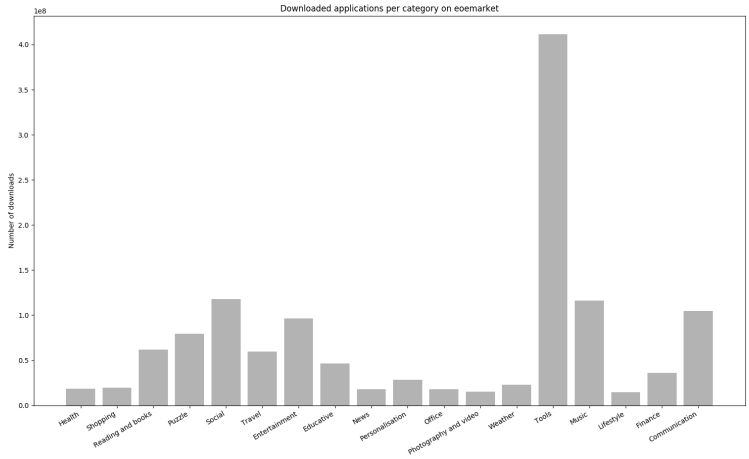
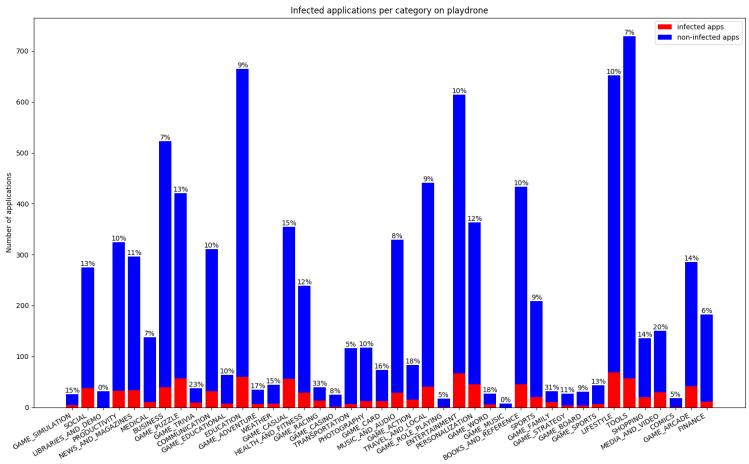
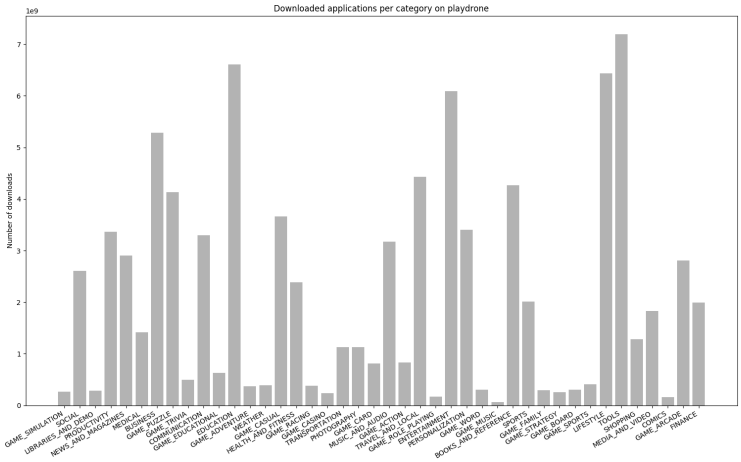


Figure 5: Downloaded applications per category on eoemarket.com



(a) Infected applications per category on Google Play store



(b) Downloaded applications per category on Google Play store

Figure 6: Analysis of Google play store categories

[2] D. R. Thomas, A.R.Beresford, A. Rice: "Security Metrics for the Android Ecosystem". Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, p. 87-98, 2015.

[3] Haoyu Wang, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jingcun Cao, Guoai Xu: "Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets" in Proc. IEEE 38th Annu. Comput. Softw. Appl. Conf., 2014, pp. 509–518.

[4] Canfora Gerardo, Medvet Eric, Mercaldo Francesco, Visaggio Corrado Aaron: "Acquiring and Analyzing App Metrics for Effective Mobile Malware Detection". In International Workshop on Security And Privacy Analytics (2016).

[5] D. Wu, C. Mao, T. Wei, H. Lee and K. Wu, "DroidMat: Android Malware Detection through Manifest and API Calls Tracing". 2012 Seventh Asia Joint Conference on Information Security, Tokyo, 2012, pp. 62-69.

[6] escalesolutions.com/blog/market-share-android-ios-other-operating-systems/

[7] statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[8] securelist.com/mobile-malware-evolution-2018/89689/