Repackaging in Third-Party Android Marketplaces

Anol Kurian Vadakkeparampil, Rohan Paranjpe, Neha Komuravelly

Dept of CISE, Project Mentor: Dr. Patrick Traynor

Herbert Wertheim College of Engineering

Introduction

There are a plethora of sources that android users can install applications from. It is crucial that the validity of these applications is put under constant examination since around 80.6% of malware tends to be repackaged applications. In this presentation we dig into the issue of app repackaging in various popular app store alternatives.

Key findings

Multiple repackaged apps were detected in prominent marketplaces that are suggested as alternatives for primary playstore on online resources.

Around 3% of apps were found to have significant variances in their signature generated as compared to reference.

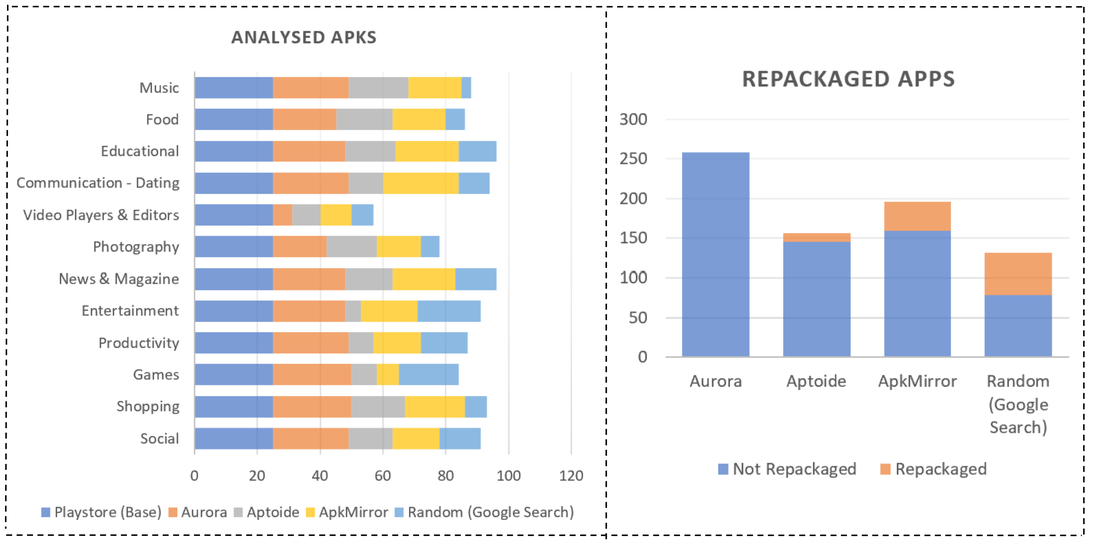
Around 7% were found to have minor discrepancies in signature matching.

Certain marketplaces have a higher contribution to this issue. (E.g. Apkmirror)

Methodology

We start by selecting our target alternative app-stores, using the most popular ones that the society uses. We use google playstore as our base and acquire apks from different marketplaces for apps of varied categories. We generate their dex codes and hash the dex using a method called T-CTPH to generate fingerprints for the apks. We then compare these fingerprints and generate a similarity score for the respective apks.

Data



We analysed a total of 1041 apks (including base-playstore) in 12 different categories from a total of four primary marketplaces, and a few random sources to balance out unavailability of certain apps on some marketplaces. We chose top 25 apps on the google-playstore for each category and their respective counterparts on other marketplaces.

Our choice of third-party marketplaces mimics the choice of the general populace as they were the ones most recommended on blogs and websites (assumption : people follow instructions on blogs and websites). Random apks were downloaded based off a google search (assumption : people download apks that pop up on the first page of a google search)

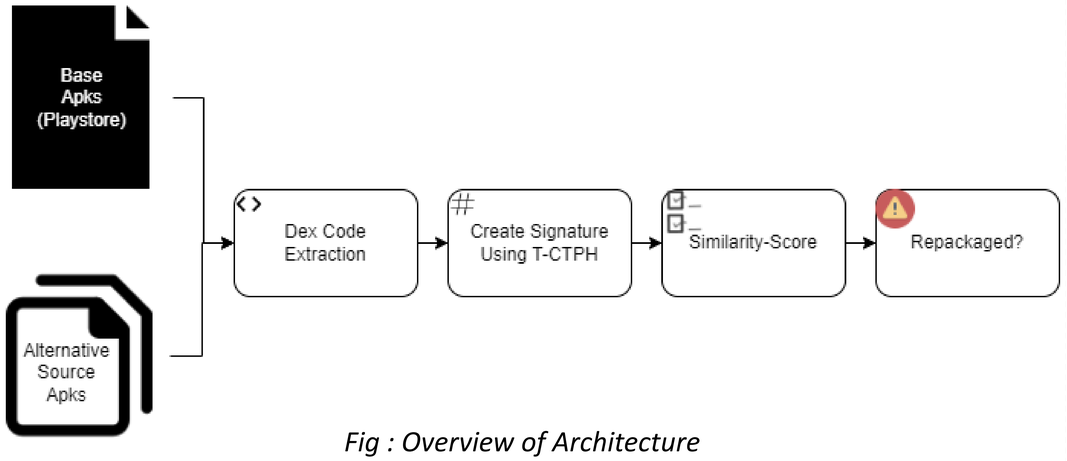


Fig : Overview of Architecture

Results

Of the 741 apks analysed with respect to their corresponding base, around 74 apks were found to be repackaged. 22 apps were found to be significantly varying and 52 had minor differences in their signature as compared to our base signature. A total of 10% repackaging has been detected from our dataset. Certain stores tend to be more susceptible to repackaged apks but still tends to be one of the most recommended sources.

Conclusions

We analysed repackaging in third-party marketplaces with a dataset of 1041 apks and were able to detect considerable repackaging in them. Based on our insights onto the distribution of these apps it is recommended to use official sources for downloading applications or introduce stricter policies on third party marketplaces.

Future Scope

The future scope for this includes extending the dataset to cover more applications and marketplaces. We would also be looking into the source code to analyse the maliciousness of these repackaged applications.

References

[1]. Zhongyuan, Qin, Pan Wan-peng, XU Ying, Feng Kerong and Yang Zhongyun. “An Efficient Scheme of Detecting Repackaged Android Applications.” (2016).

[2]. Wu Zhou et al, Detecting repackaged smartphone applications in third-party android marketplaces. (CODASPY '12). Association for Computing Machinery, New York, NY, USA, 317–326. https://doi.org/10.1145/2133601.2133640