TECHNICAL SURVEY

Preview of " An Analysis of Pre-installed Android Software and Risks for Users' Privacy", an study by IMDEA NETWORKS and UC3M

Authors: Julien Gamba (IMDEA Networks Institute), Mohammed Rashed (UC3M), Abbas Razaghpanah (Stony Brook University, USA), Juan Tapiador (UC3M) Narseo Vallina Rodriguez (IMDEA Networks Institute)

In this technical survey an insight is made to the paper *An Analysis of Pre-installed Android Software* written down by the IAG groups of the IMDEA Networks Institute and COSEC of the Carlos III University of Madrid on the analysis of pre-installed applications (apps) in devices that use the Android operating system.

The study will be published in the next 41th IEEE Symposium on Security and Privacy, can be found https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf Due to its implications in relation to personal data protection and privacy, it is of great interest to the Spanish Data Protection Authority (AEPD) and to all possible agents involved in the processing of personal data performed in mobile devices with Android operating system; both from the conception of digital products and services and throughout the life cycle of such products and services, with regard to the application of data protection principles *data protection by design and data protection by default*.

AEPD contributes to the dissemination of the paper which is considered of general interest for the entire community involved in the development and distribution of such devices, services and products of the digital economy. In the end, this paper is expected to contribute to the establishment of guarantees for the effective application of the right to data protection of those whose data and personal information may be subject to processing.

Moreover, AEPD expects to contribute on the whole to the dissemination of scientific work related to the processing of personal data on which the digital economy is based in order to facilitate the application of the general principles of the RGPD and facilitate the necessary prevention to guarantee the rights and freedoms of people, collaborating with technology managers and professionals to the implementation of such principles, and at the same time promoting the scientific research in of data protection and privacy field.

The conclusions set out in the paper correspond only to the authors

and are of a scientific nature without entering into legal considerations and without prejudice to possible actions that may arise from the powers and coherence framework established by the GDPR in relation to possible personal data processing activities that may exist in this environment.

ANDROID

The *open-source* version of Android maintained by Google, known as Android Open Source Project (AOSP), is adapted by Android smart device manufacturers and operators in the telecommunications industry in order to improve the performance of their products and add functionality that provides added value and thus differentiate them in the market.

Google has developed a program that defines the requirements that the modified operating system must meet to remain compatible with Google services [1] and maintain a public list of certified vendors [2]..

As a result, currently all sellers of Android devices distribute their own modified versions of Android in which they also include software (apps) developed by themselves or by third parties, among which are mobile operators, social networks or Internet advertising services. These are the well-known pre-installed applications on which the average user does not have the knowledge to uninstall or remove from the device and he is not able to technically verify the application of the data protection principles by default and by design.

In principle, Android implements a system of permissions to allow the user to directly control the access of the apps to system resources (e.g., GPS) and personal data (e.g., contact list) [7,8]. Android allows the user to control access to these resources during the installation of the apps from Google Play (or through the configuration of the system once installed). However, pre-installed apps run with privileged system permissions and without possibility, in most cases, of being uninstalled from the system in a simple way. This gives them great access privileges to protected resources for pre-installed software, as well as many limitations for users to exercise its control over it. These privileges extend to embedded third-party libraries in pre-installed apps for advertising and user monitoring purposes.

A priori, it shows a lack of transparency in the process by which an app is pre-installed on a specific Android device. The general press has questioned several sellers of Android devices for exhibiting abusive behaviour, introducing vulnerabilities, as well as the existence of non-transparent agreements with large Internet advertising companies [3,4,5], with manufacturers and distributors of these devices, such issue could be now ratified by this analysis.

The absence of an academic and systematic analysis on the risks of the software pre-installed on Android devices has motivated the execution of this

study that comes to lay down the foundations for the improvement of the quality of these products and services that will ultimately result in the trust of the end user in them thanks to the guarantees for their right to data protection, that is, data protection as a matter of trust in the services and products of the digital economy for citizens.

RESEARCH AIMS AND METHODOLOGY

The efforts of the research team represented by the authors have focused mainly on shedding light on three axes of work:

1. To identify and investigate the agents present in pre-installed software on Android and that take advantage of privileged access to system resources to obtain users personal data at scale;
2. To reveal possible commercial agreements between Android device sellers and third parties, including organizations specialized in monitoring and tracking users, and providing advertising resources in Internet;
3. To detect and analyse vulnerabilities and other opaque or questionable practices.

The study covers more than 82,000 pre-installed apps on more than 1,700 Android devices manufactured by 214 brands. The samples have been obtained, with the informed consent of the interested parties, thanks to the voluntary and unselfish collaboration of Android users distributed all over the world. Next, the obtained apps have been analysed by the research team with advanced software analysis techniques. More than 91% of the analysed apps are not publicly available on Google Play, including software developed by large companies.

In addition, a fourth aspect has been analysed:

4. Transparency in the information provided to a user at the time of starting his mobile device in relation to the installation of apps and data collection.

For this last aspect, six brand new Android devices from popular suppliers were purchased directly from a wholesaler and the information provided was analysed, as well as consent forms and terms of use shown to the user from the moment the device was initially powered on and, therefore, starting of the manufacturer's base configuration.

RESEARCH RESULTS

The main findings of the analysis are summarized in the following points:

- Apart from the standard permissions defined in Android and under user control, more than 4,845 permissions owned or customized by vendors ("custom permissions") and exposed by pre-installed apps have been identified. This type of permissions allows apps published on Google Play to bypass the Android permission model to access user data without requiring its consent when installing a new app.

- This permissions scheme is used by device developers, mobile operators, user monitoring and advertising services, content providers, social networks, communication services, or industrial consortiums, among many other actors.
- About the types of organizations responsible for the development of pre-installed apps, more than 1,200 companies have been identified, as well as the presence of more than 11,000 third-party libraries (SDKs) included in them [6]. Most of the libraries are related to online advertising and monitoring services for commercial purposes. This analysis reveals the existence of a complex ecosystem of developers and commercial agreements between firms for the monetization of mobile services.
- A thorough analysis of the behaviour of the 50% of the identified apps reveals that a significant fraction of them has a potentially malicious or unwanted behaviour. For example, some user monitoring and analytics services combine device telemetry with other information such as user's geolocation, contacts, identities, emails and call history. It has been found, among others:
    - Malware samples known as Xynyin, SnowFox, Rootkit, Triada y Ztorg;
    - Generic Trojans that allow silent installation of software or remote control of the device (rooted)
    - Pre-installed software that would facilitate potentially fraudulent practices through the sending of SMS messages to premium numbers, the promotion of apps to attract new users and online advertising.
- About the information provided during the initialization of a new device, of the six Android devices studied, in three of them no privacy policy was found except for the Android standard terms of use. The remaining three showed a privacy policy in which the collection of data for analysis is mentioned, but no information was found on whether this data is collected by third parties and on the specific purposes.

PRELIMINARY CONCLUSIONS

This research shows that the open-source Android model and the current monetization model of mobile devices and applications enable many actors to monitor and obtain personal information from users at the operating system level through pre-installed software.

End user is not aware of the presence of such actors in their Android terminals and the implications that these practices have on their personal data protection.

The mere presence of this software with operating system privileges makes it difficult to remove it without being an expert user. On the other hand, the amount

of existing permissions is far from what could be managed humanely and reveals a deficit of transparency in the applications and the Android operating system itself, by only showing the user a partial permissions list which is far from the real one, thus limiting user decision-making ability to manage its personal information and exercise its right to data protection.

From this study, also complex commercial relationships between actors are deduced, which make up the Android monetization ecosystem and the online advertising industry.

Finally, and in relation to the application of the principles of Data Protection by Design and by Default prescribed in the General Data Protection Regulation, it is essential that developers and mobile device sellers know this circumstance and apply said principles in order to offer the maximum guarantees of protection to its users.

BIBLIOGRAPHICAL REFERENCES

[1] Android Compatibility Program.
https://source.android.com/compatibility/overview
[2] Android Certificate Partners.
https://www.android.com/certified/
[3] "Facebook Gave Device Makers Deep Access to Data on Users and Friends". New York Times, 2018.
https://www.nytimes.com/interactive/2018/06/03/technology/facebookdevice-partners-users-friends-data.html.
[4] "Oneplus device root exploit: Backdoor in engineermode app for diagnostics mode". Now Secure. 2017.
https://www.nowsecure.com/blog/2017/11/14/oneplus-device-rootexploit-backdoor-engineermode-app-diagnostics-mode/
[5] "App Traps: How Cheap Smartphones Siphon User Data in Developing Countries". Wall Street Journal. 2018.
https://www.wsj.com/articles/app-traps-how-cheap-smartphones-helpthemselves-
to-user-data-1530788404.
[6] Abbas Razagpanah, et. al. ,"Apps, trackers, privacy, and regulators:
A global study of the mobile tracking ecosystem". In Proceedings of NDSS (2018).
[7] K.W. Au, et. al "Pscout: analyzing the android permission specification".
In Proceedings of the 2012 ACM Conference on Computer and Communications
Security (2012), ACM, pp. 217–228.
[8] Adrienne Porter-Felt, et al. "Android permissions demystified". In Proceedings of the 18th ACM Conference on Computer and Communications Security (2011), ACM, pp. 627–638