Study analyzes pre-installed software on Android devices and its privacy risks for users

20 March 2019

Juan Tapiador from Universidad Carlos III de Madrid and Narseo Vallina-Rodríguez from IMDEA Networks Institute and the International Computer Science Institute (ICSI) , are co-authors of this study together with other three researchers, one of which is from Stony Brook University of New York (USA). Credit: IMDEA Networks Institute

Universidad Carlos III de Madrid (UC3M) and the IMDEA Networks Institute, in collaboration with the International Computer Science Institute (ICSI) at Berkeley (USA) and Stony Brook University of New York (USA), have carried out a study that encompasses 82,000 pre-installed apps in more than 1,700 devices manufactured by 214 brands, revealing the existence of a complex ecosystem of manufacturers, mobile operators, app developers and providers, with a wide network of relationships between them. This includes specialized organizations in user monitoring and tracking and in providing Internet advertising. Many of the pre-installed apps facilitate access to privileged data and resources, without the average user being aware of their presence or being able to uninstall them.

The study shows, on the one hand, that the permission model on the Android operating system and its apps allow a large number of actors to track and obtain personal user information. At the same time, it reveals that the end user is not aware of these actors in the Android terminals or of the implications that this practice could have on their privacy. Furthermore, the presence of this privileged software in the system makes it difficult to eliminate it if one is not an expert user.

These results are detailed out in an article that will be made public on April 1 and which will be presented at one of the main cybersecurity and privacy conferences worldwide, the 41st IEEE Symposium on Security and Privacy, California (USA) under the title An Analysis of Pre-installed Android Software. The Agencia Española de Protección de Datos- AEPD (Spanish Data Protection Agency), which has contributed to the dissemination of this study because of the massive impact of the results on citizen privacy, will present the results before the European Commission for Data Protection.

Other findings

In addition to the standard permissions defined in Android and that can be controlled by the user, the researchers have identified more than 4,845 owner or personalized permissions by different actors in the manufacture and distribution of the terminals. This type of permission allows the apps advertised on Google Play to evade Android's permission model to access user data without requiring their consent upon installation of a new app.

As for pre-installed apps on devices, 1,200 developers have been identified behind the pre-installed software, as well as the presence of more than 11,000 third party libraries (SDKs) included in

the same. An important part of the libraries is related to advertising services and online tracking for commercial purposes. These pre-installed apps are executed with privileged permission and without being able, in the majority of cases, to be uninstalled from the system. An exhaustive analysis of the behavior of 50% of the identified apps reveal that many of them display potentially dangerous or undesired behavior.

In relation to the information offered upon logging into a new terminal, the lack of the apps transparency and of the Android operating system itself is brought to light, upon showing the user a list of permissions different from the real ones, thereby limiting capacity for decision-making regarding personal data management.

AEPD course of action

In accordance with a press release from the AEPD, this national agency will present this study and its conclusions to the working subgroups of the European Commission for Data Protection (ECDP), a European Union entity that forms a part of the Agency, together with other European data protection authorities and the European Supervisor. Among the functions of the ECDP is the fostering of cooperation among data protection agencies.

The Agency includes in the second central axis of its Strategic Plan (Innovation and Data Protection) the establishment of channels of collaboration with research groups, industry, and developers, with the objective of fomenting confidence in the digital economy in line with what is set out in the General Data Protection Regulation (GDPR). According to the Spanish Data Protection Agency, this study contributes to enabling manufacturers, developers and distributors to apply the principles of Privacy by Default and Design established in the GDPR and aimed at safeguarding the rights and freedom of individuals. Dissemination of the study undertaken by IMDEA Networks and UC3M forms part of these actions, independent of possible actions that may result from the powers and the coherent framework established by the GDPR.

More information: Julien Gamba et al. An Analysis of Pre-installed Android Software.

haystack.mobi/papers/preinstal … droidSW_preprint.pdf
To appear in the 41st IEEE Symposium on Security and Privacy (IEEE S&P 2020)

Provided by IMDEA Networks Institute