PRESS RELEASE
NOTA DE PRENSA

Madrid, Spain, January 29, 2020

AEPD and CNIL award their data protection prizes to a team including researchers from IMDEA Networks

The award-winning article is “An Analysis of Pre-installed Android Software” by Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador and Narseo Vallina-Rodriguez

The article, “An Analysis of Pre-installed Android Software” by Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador and Narseo Vallina-Rodriguez, has received two prestigious awards this month: one from the Spanish Data Protection Agency (AEPD) and another from the CNIL (French Data Protection Authority) and Inria. The study has huge social impact as it reveals the privacy and security issues associated with pre-installed software on Android devices and their supply chain.

On 28 January, the AEPD chose the Spanish Senate as the setting to award the “Emilio Aced Personal Data Protection Research” prize to this team of researchers from IMDEA Networks Institute (an institution promoted by the Community of Madrid), the Universidad Carlos III de Madrid, the International Computer Science Institute (ICSI) at Berkeley (USA) and Stony Brook University of New York (USA). On 18 December 2019, the agency gave the '2019 Data Protection Awards', which recognize work that promotes knowledge, research and the dissemination of the fundamental right to data protection. At the awards ceremony, the AEPD's “The Story Behind” campaign was also presented.

A few days earlier, on 22 January, the scientists received the CNIL-Inria Privacy Award for the same paper at the international conference CPDP 2020 - Data Protection and Artificial Intelligence held in Brussels. Julien Gamba presented this study, which has also been accepted for publication at the IEEE Symposium on Security and Privacy 2020 (USA). It is a truly in-depth article, covering more than 82,000 apps pre-installed in more than 1,700 devices manufactured by 214 brands. The research shows many of the pre-installed applications provide privileged access to data and system resources although the average user would be unable to uninstall them.

“Our results show how opaque the Android device supply chain is to users and how poorly understood it is by researchers. The vast majority of pre-installed applications are not public, making them difficult to collect and analyze: this is partly because they have escaped the scrutiny of the scientific community for a long time. We came up with an innovative solution to collect a large data set of pre-installed applications and found that there were a large number of companies involved in creating Android devices, including those with data-driven business models, which could put users' privacy and security at risk,” explains Gamba, a PhD student at IMDEA Networks and the study's principal investigator.

Key findings

Apart from the standard permissions defined in Android and that can be controlled by the user, researchers have identified more than 4,845 proprietary or customized permissions by those

involved in the manufacture and distribution of the terminals. These types of permissions allow apps published in Google Play to bypass the Android permission model to access user data without requiring users' consent when installing a new app.

As for the apps pre-installed on the devices, more than 1,200 developers have been identified behind the pre-installed software, along with the presence of more than 11,000 third party libraries (SDKs) included in the apps. Many of the libraries are related to online advertising and monitoring services for commercial purposes. These pre-installed apps are executed with privileged permissions and without the possibility, in most cases, of being uninstalled from the system. An exhaustive analysis of the behavior of 50% of the identified apps reveals that many of them exhibit potentially dangerous or unwanted behavior.

There is a lack of transparency in the apps and the Android operating system itself in the information offered to the user when initiating a new terminal. The user is shown a list of permissions that differs from the real one, thereby limiting the user's decision capacity in managing their personal information.

According to Gamba, "the real challenge is to identify with certainty the stakeholders in the supply chain". While this study has shed some light on this ecosystem and has uncovered many supply chain stakeholders, "there are still many ways to avoid detection". "We are currently working on improving state-of-the-art tools that will enable us to design ways to uncover the presence of all these stakeholders and eventually to paint a complete picture of the Android supply chain," says the IMDEA Networks researcher.

Source(s): IMDEA Networks Institute

–END–

Traducción al español:
/noticias/2020/aepd-cnil-otorgan-sus-premios-proteccion-datos-un-equipo-que-participan
Original source:
/news/2020/aepd-and-cnil-award-their-data-protection-prizes-team-including-researchers

About Us

IMDEA Networks Institute is a **research organization on computer and communication networks** whose multinational team is engaged in cutting-edge fundamental science and technology. As a growing, English-speaking institute located in Madrid, Spain, IMDEA Networks offers a unique opportunity for pioneering scientists to develop their ideas. IMDEA Networks has established itself internationally at the forefront in the **development of future network principles and technologies.** Our **team** of highly-reputed researchers is designing and creating today the networks of tomorrow.

Some keywords that define us: *5G, Big Data, blockchains and distributed ledgers, cloud computing, content-delivery networks, data analytics, energy-efficient networks, fog and edge computing, indoor positioning, Internet of Things (IoT), machine learning, millimeter-wave communication, mobile computing, network economics, network measurements, network security, networked systems, network protocols and algorithms, network virtualization (software defined networks – SDN and network function virtualization – NFV), privacy, social networks, underwater networks, vehicular networks, wireless networks and more…*

28918 Leganés (Madrid) Spain
Avda. del Mar Mediterráneo, 22
mediarelations.networks@imdea.org
www.networks.imdea.org
Twitter: @IMDEA_Networks | LinkedIn | Facebook | Instagram | Flickr | YouTube