Mobile health applications put the personal data of millions of users at risk

February 21 2018

80 percent of the most popular health applications available on Android do not comply with standards intended to prevent the misuse and dissemination of user data. This is the finding of a European study started in 2016 involving Agusti Solanas and Constantinos Patsakis. The research has brought to light evidence of serious security problems regarding the 20 most popular applications on the internet. The research consisted of analysing the security problems, communicating them to the software developers and then checking them to see if they had been resolved.

The applications chosen by the researchers had been downloaded between 100,000 and 10 million times and had a minimum rating of 3.5 out of 5. To analyse their levels of security, the researchers intercepted, stored and monitored private data relating to users' health problems, illnesses and medical records. The researchers analysed how the applications communicated, how they stored information, which permissions they required to operate, and how they handled the data. The results showed the existence of serious security problems in the handling of user data.

Only 20 percent of the applications stored the data on the smartphone, and one in two requested and administered passwords without using a secure connection. The researchers also found that 50 percent of the applications shared data with third parties, including text and multimedia content.

More than half transferred users' health data via HTTP links, which means that anybody with access could get their hands on the data. 20 percent of the applications did not inform the user of any privacy policy or the content was not available in English, the language of the application. Others requested access to geolocation, microphones, cameras, contact lists, external storage cards and Bluetooth, even though the application did not need access to these data to operate.

On completing the analysis, the researchers contacted the software developers to inform them of the security problems. After waiting for a given period, they then analysed the same parameters and found that although some of the security issues had been fixed (e.g. insecure health data transfers or the ability to identify users via insecure data transfers to third parties), other problems such as data leaks regarding the use of the application had not been resolved.

More information: Achilleas Papageorgiou et al. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice, *IEEE Access* (2018). DOI: 10.1109/ACCESS.2018.2799522

Provided by Universitat Rovira i Virgili