PHYS.ORG

App data vulnerability threatens millions of users

May 29 2015

Users should take care what kind of data they trust their apps with. Credit: Fraunhofer SIT

Researchers of the Technische Universität Darmstadt and Fraunhofer SIT have investigated Cloud databases and established: developers wrongly use authentications for cloud services thereby threatening millions of user accounts which become susceptible to attack.

Technische Universität Darmstadt and Fraunhofer SIT have investigated cloud databases like Facebook's Parse and Amazon's AWS and found 56 million sets of unprotected data.

The researchers found email addresses, passwords, health records and other sensitive information of app users, which may be easily stolen and often manipulated. App developers use cloud databases to store user data but apparently ignore the security recommendation given by the Cloud providers. As a result, many user accounts are threatened by identity theft and other cybercrimes.

"Therefore users should take care what kind of data they trust their apps with", says Prof. Eric Bodden, the leader of the joint research team. Further information about the vulnerability has been provided by the researchers online.

Different methods of authentication

Many smartphone apps store user information in Cloud databases, for instance to ease synchronization between Android, and iOS apps. Cloud providers offer different authentication methods according to the information's sensitivity.

The weakest form of authentication, meant to identify rather than to protect the data, uses a simple API-token, a number embedded into the App's code. With current tools, however, attackers can easily extract those tokens and not only read the data, but often even manipulate it. Attackers could, for example, sell email addresses on the underground market, blackmail users, deface websites or insert malicious code to spread malware or build botnets.

To properly protect private data, apps must implement an access-control scheme. However, the tests show that the vast majority of apps do not use such access control. Focusing on apps from Google's Play Store and Apple's App Store, the scientists have scanned 750.000 apps using different internally developed analysis frameworks including for example Fraunhofer's Appicaptor. With the help of these expert tools the scientists were able to identify apps using the weak authentication and started an in-depth analysis of selected apps. During the investigation it turned out that many data items contained private information, for example verified email addresses, full user names or information about psychological illnesses.

Developers must take action

"Due to legal restrictions and the huge amount of suspicious apps, we could only inspect a small number in detail", says Prof. Eric Bodden. "However, our findings and the nature of the problem indicate that an enormous amount of app-related information is open to identity theft or even manipulation.

" When the scientists discovered the problem, they immediately informed the cloud providers and the German Federal Office for Information Security (BSI). "With Amazon's and Facebook's help we also informed the developers of the respective apps and they really are the ones who need to take action because they underestimated the danger", says Bodden.

Provided by Technische Universitat Darmstadt

Citation: App data vulnerability threatens millions of users (2015, May 29) retrieved 24 April 2024 from https://phys.org/news/2015-05-app-vulnerability-threatens-millions-users.html