PHYS.ORG

Web-based services that store too much personal data

June 19 2015, by Sarah Perrin

Credit: Thinkstock

Photos, videos, PDF documents and location data: the permissions requested by some apps give them access to more information than users are aware of. EPFL researchers have come up with a tool to better follow and manage these risks.

Exactly what personal data are we putting on the web in the era of the cloud? Often much more than we want or even imagine. That is what researchers at EPFL's Distributed Information Systems Laboratory (LSIR) have discovered. They have developed a tool, PrivySeal, that informs users exactly what data they are agreeing to share when they accept the permissions of various apps available on the internet.

Popular websites like Google Drive, Dropbox and OneDrive generally have strict and longstanding privacy rules. The only catch is that these websites are often used as a platform for related apps that provide cloud-based services like photo editing, PDF merging and editing, content searching and analysis, to name just a few.

"We want to let users know the risks they take when using these services and give them a better way to assess these risks," said Hamza Harkous, a PhD candidate at the LSIR and the lead researcher on this project.

Where, when and with whom?

The "Accept" that users mechanically click so they can use an app to touch up a photo, for example, can open the door to the users' entire photo collection – and to the sometimes very detailed date- and location-related information tagged to the photos. Someone could use that to figure out where and with whom the user had a drink on Tuesday at 6pm or where the user went on vacation last summer. Blindly accepting the permissions of a document filing service can also provide access to other types of data. And as a result, a third party could see who the user's main collaborators were and what topics were discussed, or figure out the user's opinions on various issues by analysing the most frequently occurring words.

"If they want to use these services, users sometimes have no other choice but to provide access to additional information, and in so doing they sacrifice some of their privacy," said Rameez Rahman, an LSIR researcher who oversaw the project. "The requested permissions often cover a much broader array of data than the services really require to function."

Prepare to be surprised!

To assess the scope of the problem, the researchers analysed more than seventy apps that are offered on two cloud platforms: Google Drive and Dropbox. The results showed that nearly half of them had this type of privacy problem.

The website developed by the LSIR researchers is now publicly accessible at privyseal.epfl.ch. It provides clear, step-by-step guidance allowing users to figure out exactly what they have authorised their apps to do and access. The personalised results are then displayed in graphical format, including different-sized circles showing the people, places and companies with which the users have the most contact on a day-to-day basis. The website also provides specific details on the consequences of various types of permission requests. After learning what data their apps can access, users can see which of the data are really needed for the apps to function properly and which are not.

Provided by Ecole Polytechnique Federale de Lausanne

Citation: Web-based services that store too much personal data (2015, June 19) retrieved 19 April 2024 from https://phys.org/news/2015-06-web-based-personal.html