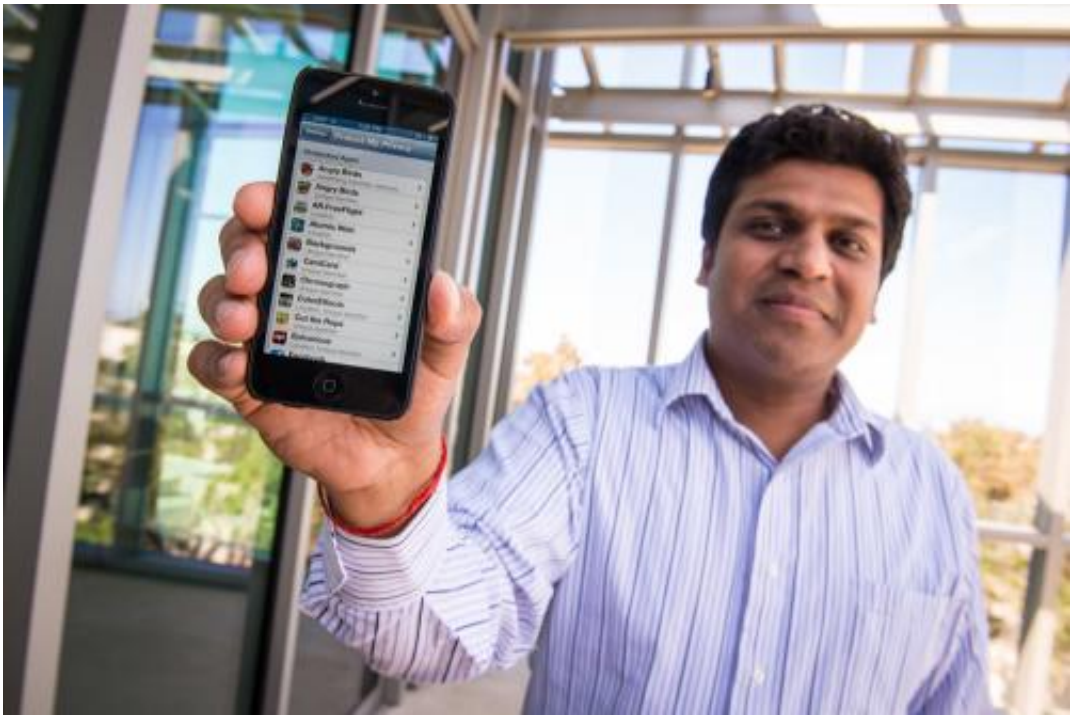
App to protect private data on iOS devices finds almost half of other apps access private data

June 20 2013



Yuvraj Agarwal, a research scientist at the University of California, San Diego, is presenting findings on June 26 at the MobiSys conference in Taipei, Taiwan. Credit: Calit2/UC San Diego

Almost half of the mobile apps running on Apple's iOS operating system access the unique identifier of the devices where they're downloaded, computer scientists at the University of California, San Diego, have

found. In addition, more than 13 percent access the devices' location and more than 6 percent the address book. The researchers developed a new app that detects what data the other apps running on an iOS device are trying to access.

The findings are based on a study of 130,000 users of jailbroken iOS devices, where users have purposefully removed restrictions that keep apps from accessing the iPhone's operating system. Most apps in the study were downloaded from Apple's App Store and access the same type of information on unlocked, jailbroken, phones and on locked phones, said Yuvraj Agarwal, a research scientist in the Department of Computer Science and Engineering at UC San Diego, who co-authored the study with fellow researcher Malcolm Hall. Agarwal will present the findings at ACM MobiSys, the premier mobile systems conference, which takes place June 25 to 28 in Taipei, Taiwan.

The findings suggest that although Apple's App Store no longer accepts new apps or app updates that access the unique identifier as of March of this year, many apps can still get a hold of that information. The unique identifier allows app vendors and advertisers to track users' behaviors across all the different apps on their devices, including iPhones, iPads and iPods. In addition, some apps can associate the unique identifier with the user's email and other personal information.

The researchers believe that it's the first time anyone has done such an extensive privacy study focused on iOS-based apps across a large user population.

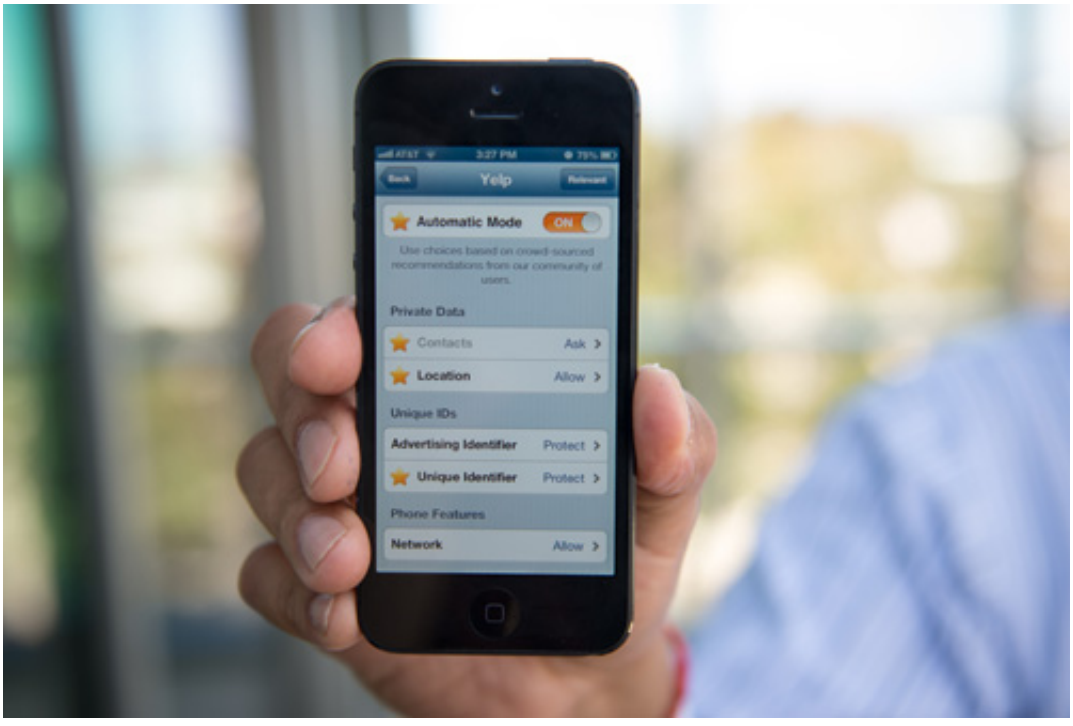
The ProtectMyPrivacy App

To carry out their study, researchers developed an app of their own, called ProtectMyPrivacy, or PMP. It lets users know what personal information the other apps on their devices are trying to access. PMP

enables users to selectively allow or deny access to this information on an app-by-app basis, based on whether they feel the apps need the information to function properly—for example, a map app needs to access the location of a device to provide driving directions. iOS devices currently notify users when apps try to access location, photos and contacts. But they do not notify users when apps access the unique identifier or music library and users can't deny access to those two pieces of information.

Since gathering data for the study, researchers have also added notifications and recommendations for when an app accesses other privacy-sensitive information, such as a devices' front and back camera, microphone and photos.

PMP also makes recommendations about whether to allow the other apps to access user data, based on an extensive crowdsourcing 'recommendation engine' that compiles the privacy decisions made by other users.



The ProtectMyPrivacy app tells users what information other apps are trying to access on iOS devices. It also makes recommendations about whether to allow or deny access. Credit: Calit2/UC San Diego

"We wanted to empower users to take control of their privacy," said Agarwal, who is also an alumnus of UC San Diego's Jacobs School of Engineering. "The choice should be in users' hands."

For locked devices, researchers are currently providing a web page that tells users which information more than 150 apps for iOS—some of the most popular—are trying to access and gives recommendations about whether to allow or deny access. The page can be viewed at http://www.protectmyprivacy.org/liveview/

For example, Facebook, the most popular app, accesses the devices' identifier, location and contacts. PMP's crowdsourcing engine recommends denying access to the identifier and contacts music, but allowing access to location.

Findings by the numbers

ProtectMyPrivacy has already been downloaded from the Cydia store by more than 130,000 users since March 2012. Its users have downloaded and used more than 225,000 unique apps from Apple's App Store. The researchers analyzed the data accessed by those apps and found that 48.1 percent of them accessed the device's unique identifier; 13.2 percent the location information; 6.2 percent the address book; and 1.6 percent the music library.

As of January 2013, Apple reported that it had sold 500 million iOS devices. Estimates of how many are jailbroken vary, but Forbes reported in February 2013 that seven million devices had been jailbroken in just four days after a new jailbreaking tool was released. Cydia, an app store that caters only to jailbroken devices, had 23 million users as of March 2013 –a sizeable portion of Apple's mobile devices.

Read the full paper here.

Recommendations to protect your privacy

Almost all of PMP's users—99 percent— voluntarily shared their privacy decisions, indicating which apps they think should be allowed—or denied—access to their privacy-sensitive data. These decisions – which are contributed anonymously – are then processed on PMP servers to generate the crowdsourced privacy recommendations shown to users. As a result, PMP is able to make recommendations for 97 percent of the 10,000 most popular iPhone apps. "We have already shown millions of recommendations, and more than two-thirds of all our recommendations are accepted by our users, showing that they really like this unique feature of PMP," said Agarwal. Users chose to deny access to one or more pieces of sensitive data for 48.1 percent of apps.

The version of PMP available in the Cydia store gives users the option to feed fictitious or anonymized information to nosy apps. Examples include an address book filled with made-up entries, a random location that may be in a completely different country, and a randomly generated unique identifier.

The researchers say that they do not recommend jailbreaking your iPhone to install PMP, because doing so could potentially leave a user open to other vulnerabilities. But in order to conduct their research, they needed to be able to intercept information about the privacy-protected

data that apps were accessing. This required low-level access to the operating system, which is not technically possible on locked, non-jailbroken, iOS devices.

Sometimes, it is not the apps themselves that access the data, but a third-party library or code contained within the apps. For example, Flixster, a popular app for movie reviews and recommendations, in its 5.2 version, was flagged for accessing some private data. Flixster contacted Agarwal and Hall to say that it does no such thing. The computer scientists did some digging and found that a third-party ad library used by the app was accessing users' address books and sending back information. "We provided feedback to the app's developers in case they are unaware that a third party library may be accessing their users' private data," recalled Hall, a visiting researcher in Agarwal's Synergy Lab at UC San Diego. He also pointed out that "an updated version of Flixster now uses another ad library that does not access this kind of information."

Agarwal and Hall tried submitting to the Apple Store a "lite" version of their app that wouldn't interact with the iOS operating system, but the app was rejected. That version would have given users information about the data specific apps access and recommendations about what to allow and deny. It would not have given users the ability to protect their data by providing fictitious information.

Agarwal will join the School of Computer Science at Carnegie Mellon University as an assistant professor in the fall.

Provided by University of California - San Diego