Researchers find phone apps sending data without notification (w/ Video)

September 29 2010, By Ashley Yeager

(PhysOrg.com) -- Publicly available cell-phone applications from application markets are releasing consumers' private information to online advertisers, according to a joint study by Intel Labs, Penn State, and Duke University.

Flicking through a wallpaper app with backgrounds of Mickey Mouse and a tropical waterfall, Peter Gilbert gets a plain, black and white text notification on his smartphone.

A third of the way down the screen it says, "Taint: Phone Number, IMEI, ICCID (sim card identifier)." The message alerts Gilbert that the

wallpaper app has sent his phone's number and other identifying information to imnet.us. Checking online, it appears the address is a website in Shenzhen, China.

The notification came from TaintDroid, a prototype extension to the Android mobile-phone platform designed to identify apps that transmit private data. The phone-based tool monitors how applications access and use privacy sensitive data, such as location, microphone, camera and phone numbers, and provides feedback within seconds of using a newly installed app.

TaintDroid recently identified that 15 of 30 randomly selected, popular, free Android Marketplace applications sent users' private information to remote advertising servers and two-thirds of the apps handled data in ambiguous ways.

Gilbert, a graduate student in computer science at Duke University, and his adviser, Landon Cox, an assistant computer science professor, helped develop TaintDroid. They collaborated with Jaeyeon Jung, Byung-Gon Chun and Anmol Sheth of Intel Labs, and William Enck and Patrick McDaniel of Penn State University.

"We found it surprising that location information was shared with ad networks without further explanation or notification," said Jung, lead co-author, along with Enck, of a new study that describes TaintDroid and the team's results.

The paper will be posted online Sept. 30 as part of the USENIX Symposium on OSDI, or Operating Systems Design and Implementation. Enck will also present the research findings Oct. 6 at the affiliated OSDI conference in Vancouver, BC.

The team found that some applications shared GPS sensor location

information with advertisement servers only when displaying ads to the user. Other applications shared location even when the user was not running the application. In some cases, location information was being shared as frequently as every 30 seconds.

The results support and expand upon a controversial SMobile Systems study published in June 2010 which found that 20 percent of the then-available 48,000 third-party applications for the Android operating system provided sensitive or private information to outside sources. In the new study, the team only monitored the Android platform, but the findings suggest that investigating other operating systems is warranted.

"We don't have the data to say that a majority of third-party apps are untrustworthy. This study, however, is a proof-of-concept to show the value of enhancing smartphone platforms to include real-time monitoring tools like TaintDroid to give users an awareness of how their information is being shared," Cox said.

Currently, mobile-phone operating systems do offer users some controls to regulate whether an application can access private information. When installing an app, like the wallpaper app, for example, Android asks the user which services and data an app may access, Gilbert says.

If the user chooses not to allow this access, the application cannot be installed. But if the user does install the app, the permission checks don't always explain how these services and data will be used. This forces users to blindly trust that applications will handle private data properly once they are installed, he says.

"The permissions don't tell the user how their data will be used, and in some cases misused," Cox adds, noting that in some cases, a privacy violation can occur where services and data are used in ways that are unexpected. Mobile anti-virus packages such as software sold by

SMobile Systems can alert users to the presence of previously identified malicious applications, but they do not provide real-time information about where applications send users' data.

TaintDroid uses a scientific technique called "dynamic taint analysis" to mark information of interest with an identifier called a "taint." The taint stays with the information when it is used, and the tracking system then monitors the movement of tainted information, such as the Internet destination of the user's information. It then sends the user a notification of the movement of information as soon as the app is closed.

"This automatic feedback gives users greater insight into what their mobile applications are doing and could help users decide whether they should consider uninstalling an app," Gilbert says.

The team plans to make TaintDroid publicly available to continue to improve smartphone application monitoring.

More information: The paper and a demo of the research prototype are at www.appanalysis.org

Provided by Pennsylvania State University

Citation: Researchers find phone apps sending data without notification (w/ Video) (2010, September 29) retrieved 19 April 2024 from https://phys.org/news/2010-09-apps-notification-video.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.