# Study: Including ads in mobile apps poses privacy, security risks

March 19 2012

Researchers from North Carolina State University have found that including ads in mobile applications (apps) poses privacy and security risks. In a recent study of 100,000 apps in the official Google Play market, researchers noticed that more than half contained so-called ad libraries. And 297 of the apps included aggressive ad libraries that were enabled to download and run code from remote servers – which raises significant privacy and security concerns.

"Running code downloaded from the Internet is problematic because the code could be anything," says Dr. Xuxian Jiang, an assistant professor of computer science at NC State and co-author of a paper describing the work. "For example, it could potentially launch a 'root exploit' attack to take control of your phone – as demonstrated in a recently discovered piece of Android malware called RootSmart."

In Google Play (formerly known as the Android Market) and other markets, many developers offer free apps. To generate revenue, these app developers incorporate "in-app ad libraries," which are provided by Google, Apple or other third-parties. These ad libraries retrieve advertisements from remote servers and run the ads on a user's smartphone periodically. Every time an ad runs, the app developer receives a payment.

This poses potential problems because the ad libraries receive the same permissions that the user granted to the app itself when it was installed – regardless of whether the user was aware he or she was granting

permissions to the ad library.

Jiang's team looked at a sample of 100,000 apps available on Google Play between March and May 2011 and examined the 100 representative ad libraries used by those apps. One significant find was that 297 of the apps (1 out of every 337 apps) used ad libraries "that made use of an unsafe mechanism to fetch and run code from the Internet – a behavior that is not necessary for their mission, yet has troubling privacy and security implications," Jiang says. But that is only the most extreme example.

Jiang's team found that 48,139 of the apps (1 in 2.1) had ad libraries that track a user's location via GPS, presumably to allow an ad library to better target ads to the user. However, 4,190 apps (1 in 23.4) used ad libraries that also allowed advertisers themselves to access a user's location via GPS. Other information accessed by some ad libraries included call logs, user phone numbers and lists of all the apps a user has stored on his or her phone.

These ad libraries pose security risks because they offer a way for third parties – including hackers – to bypass existing Android security efforts. Specifically, the app itself may be harmless, so it won't trigger any security concerns. But the app's ad library may download harmful or invasive code after installation.

"To limit exposure to these risks, we need to isolate ad libraries from apps and make sure they don't have the same permissions," Jiang says. "The current model of directly embedding ad libraries in mobile apps does make it convenient for app developers, but also fundamentally introduces privacy and security risks. The best solution would be for Google, Apple and other mobile platform providers to take the lead in providing effective ad-isolation mechanisms."

The paper, "Unsafe Exposure Analysis of Mobile In-App Advertisements," was co-authored by Jiang; NC State Ph.D. students Michael Grace and Wu Zhou; and Dr. Ahmad-Reza Sadeghi of the Technical University Darmstadt. The paper will be presented April 17 at the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks in Tucson. The research was supported by the National Science Foundation.

Provided by North Carolina State University