Researchers find some smartphone models more vulnerable to attack

November 30 2011

New research from North Carolina State University shows that some smartphones specifically designed to support the Android mobile platform have incorporated additional features that can be used by hackers to bypass Android's security features, making them more vulnerable to attack. Android has the largest share of the smartphone market in the U.S.

"Some of these pre-loaded applications, or features, are designed to make the smartphones more user-friendly, such as features that notify you of missed calls or text messages," says Dr. Xuxian Jiang, an assistant professor of computer science at NC State and co-author of a paper describing the research. "The problem is that these pre-loaded apps are built on top of the existing Android architecture in such a way as to create potential 'backdoors' that can be used to give third-parties direct access to personal information or other phone features."

In essence, these pre-loaded apps can be easily tricked by hackers. For example, these "backdoors" can be used to record your phone calls, send text messages to premium numbers that will charge your account or even completely wipe out all of your settings.

The researchers have tested eight different smartphone models, including two "reference implementations" that were loaded only with Google's baseline Android software. "Google's reference implementations and the Motorola Droid were basically clean," Jiang says. "No real problems there."

However, five other models did not fare as well. HTC's Legend, EVO 4G and Wildfire S, Motorola's Droid X and Samsung's Epic 4G all had significant vulnerabilities – with the EVO 4G displaying the most vulnerabilities.

The researchers notified manufacturers of the vulnerabilities as soon as they were discovered, earlier this year.

"If you have one of these phones, your best bet to protect yourself moving forward is to make sure you accept security updates from your vendor," Jiang says. "And avoid installing any apps that you don't trust completely."

Researchers now plan to test these vulnerabilities in other smartphone models and determine whether third-party firmware has similar vulnerabilities.

More information: The paper, "Systematic Detection of Capability Leaks in Stock Android Smartphones," will be presented Feb. 7, 2012, at the 19th Network and Distributed System Security Symposium in San Diego, Calif.

Provided by North Carolina State University