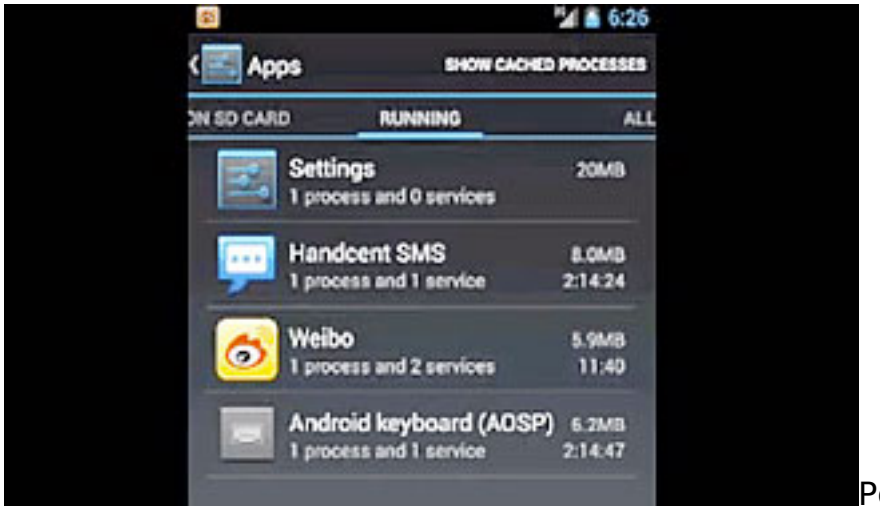
Security holes in smartphone apps

UC Davis



Popular texting, messaging and microblog apps developed for the Android smartphone have security flaws that could expose private information or allow forged fraudulent messages to be posted, according to researchers at the University of California, Davis.

Zhendong Su, professor of computer science, said that his team has notified the app developers of the problems, although it has not yet had a response.

The security flaws were identified by graduate student Dennis (Liang) Xu, who collected about 120,000 free apps from the Android marketplace. The researchers focused initially on the Android platform, which has about a half-billion users worldwide. Android is quite different from Apple's iOS platform, but there may well be similar problems with iPhone apps, Xu said.

The victim would first have to download a piece of malicious code onto their phone. This could be disguised as or hidden in a useful app, or attached to a "phishing" e-mail or Web link. The malicious code would then invade the vulnerable programs.

The programs were left vulnerable because their developers inadvertently left parts of the code public that should have been locked up, Xu said.

"It's a developer error," Xu said. "This code was intended to be private but they left it public."

Su and Xu, with UC Davis graduate student Fangqi Sun and visiting scholar Linfeng Liu, Xi'an Jiatong University, China, found that many of the apps they surveyed had potential vulnerabilities. They looked closely at a handful of major applications that turned out to have serious security flaws.

Handcent SMS, for example, is a popular text-messaging app that allows users to place some text messages in a private, password-protected inbox. Xu found that it

is possible for an attacker to access and read personal information from the app, including "private" messages.

WeChat is an instant messaging service popular in China and similar to the Yahoo and AOL instant messengers. The service normally runs in the background on a user's phone and sends notifications when messages are received. Xu discovered a way for malicious code to turn off the WeChat background service, so a user would think the service is still working when it is not.

Weibo is a hugely popular microblog service that has been described as the Chinese equivalent of Twitter. But its Android client is vulnerable, and it is possible for malicious code to forge and post fraudulent messages, Xu said.

The researchers have submitted a paper on the work to the Systems, Programming, Languages and Applications: Software for Humanity (SPLASH) 2013 conference to be held in Indianapolis this October.

Source: http://news.ucdavis.edu/search/news_detail.lasso?id=10556 [1]

Source URL (retrieved on *12/13/2013 - 1:22pm*):
http://www.ecnmag.com/news/2013/04/security-holes-smartphone-apps

Links:
[1] http://news.ucdavis.edu/search/news_detail.lasso?id=10556