Researchers point out ways to circumvent Google's Bouncer (w/ Video)

June 7 2012, by Bob Yirka

(Phys.org) -- Back in February, Google announced that it had added a security program called Bouncer to its Android Market, a site similar to Apple's iTunes, that would test applications that had been uploaded to the site, in an attempt to keep out those that contain malware. In the announcement, Google also said that Bouncer had been running for several months and that because of it, apps with malware uploaded to Android Market, which is now called Google Play, were down forty percent. Unfortunately, if that number is correct, it's likely to change soon as two security analysts, Charlie Miller and Jon Oberheide have not only found some very serious security problems with Bouncer, but have created a video and posted it on YouTube showing exactly how to take advantage of the lapse.

Miller and Oberheide explain that the way Bouncer works is by creating a virtual phone environment every time an app is uploaded to Google Play. It's in that environment that Bouncer runs and tests the app in various ways to see if it can detect the presence of any malware. Unfortunately, as the two found, Bouncer only tests for five minutes. Any app that waits till after that time period has lapsed to carry out its nefarious functions will get a clean bill of health.

The duo discovered this flaw in Bouncer by creating an app that automatically connects to a server under their control, which allowed them to run Linux commands on an Android phone. Then, they created a false Google Play developer account and uploaded the app. Once it ran in the simulator, they were able to execute commands to find out how

Bouncer worked and then to use that information to find weaknesses.

In so doing, they also found that Google had created just a single fake user account, email address, and two photo images to use for its testing purposes. If an app with malware tried to touch any of those, it was "bounced." Unfortunately, using such a limited set of test information allows those working to subvert the system an easy means of identifying if they are running in a simulation or on a real phone. If it's the simulation, then they can just do nothing so they won't be detected.

The two researchers say there are other security holes they've discovered as well and have been in contact with Google to let them know what they've found and will be outlining their findings at this week's SummerCon conference in New York.