Security firm finds smartphones lacking in security

August 10 2011, by Bob Yirka

(PhysOrg.com) -- viaForensics, a computer security firm, has undertaken an exhaustive study to determine just how secure data is on smartphones; their results show that data such as login names, passwords, account numbers and in some cases even social security numbers, aren't nearly as secure as most people would assume. The company has produced both a white paper detailing its results (including providing results for actual apps by name) and a report on its website detailing its findings.

The purpose of the report, the company says, is to give owner/users of smartphones (and tablets, etc.) a more clear understanding of the risks involved when using apps on their smartphones to perform various Internet related activities. They broke such apps into four broad categories: Financial, Social Networking, Productivity and Retail. They then set up a grading system of Pass, Warm and Fail. A Passing grade, obviously enough meant that "secure" data on the device was either not present or was encrypted. *Warm* meant that data was found, but its presence didn't put the user (in viaForensics opinion) at risk. *Fail* meant login names, passwords or other data were found and recovered from the device.

Overall, the report shows that Financial apps (Fail-25% Warm-31% Pass-44%) were the most secure, while Social Networking (Fail-74% Warm-26% Pass-0%) apps were the least; while Productivity (Fail-43% Warm-49% Pass-9%) and Retail (Fail-14% Warm-86% Pass-0%) apps fell in the middle. Though that might not be saying much since so many

apps overall (Fail-39% Warm-44% Pass-17%) were either Warm or failed to secure customer data from financial or identity theft.

In addition, the authors of the report found that 76% of apps stored usernames with no encryption, and 10% didn't encrypt passwords either.

To test the devices and apps, viaForensics tested 100 popular apps on running on Apple's iOS and Google's Android platform. They installed the apps on the phones via app stores and filled each with normal data. They also used real financial accounts.
In the report, the authors note that the most prevalent piece of user data they were able to retrieve was login names, which they point out, means that if someone were to steal the phone, or hack their way in via malware, they'd have half the puzzle of breaking into user data half-solved.

Finally, while the authors do mention that once a phone is lost or stolen, the person who finds it would have to have to do some digging to find such sensitive data, they don't mention the fact that most people who find a lost phone, or steal one for that matter, wouldn't have the foggiest idea how to dig for such sensitive data, thus the risk might not be as great as indicated; this fact does not mean that apps makers are off the hook though of course, as clearly they have some very serious explaining to do.