Security in Smartphones

Martin Bakal, IBM Rational (www.IBM.com/Rational)

The smartphone market is expected to increase 24.5% in 2011, as projected by IDC [1]. Managing security will be a big concern and key area of focus for most mobile companies going forward. Companies who address this concern successfully will most likely capture the market share.

People view their bank account information, medical records and other sensitive data on their mobile devices. With multiple ways to access this data, the key concern is how to make it safer. This is especially true as the demand and expectation for rich content is driving development teams to even shorter product cycles.

In order to understand how to protect the data, first we have to understand the potential holes in the overall system. One source of potential vulnerability is a website from which a mobile application user accesses data or downloads applications. The site could be corrupted or corrupt the applications residing on the device before data is downloaded. Alternatively, applications themselves could have hidden trojans inside them. Another way security is compromised is by data being passed over public, wireless connections. Any unencrypted data can be read by anyone. One of the biggest risks for mobile devices is that one rogue application on the device may “snoop” into data owned by the other applications running on the device.

But how do you account for potential security holes and design in protection? Most projects only focus on security as a testing issue, i.e. design and develop the system and then test it to look for potential vulnerability. While security testing is an important step and needs to be part of the overall strategy, it is not sufficient.

Project developers need to think about designing with security in mind from the beginning. This means taking a good look at how you will develop each component and where the interfaces to the outside world are. Model the system and understand what data will be passed through those interfaces. Then you can make decisions on where protections need to be put in place; when encryption needs to be added; and all the other facets of a good complete product security.

As you design each component you also need to use static code analysis tools to see if and where the code poses any security risk. This analysis can be executed during the source code check-in process. Once you perform static code vulnerability analysis, you can use a dynamic “black-box” scanning tool to check the web site where the application resides becomes another critical factor.

All of this does take a little extra time and planning - which is why it is critical to reuse this same design in other products lines you build through a good Product Line Engineering (PLE) strategy. A good PLE strategy allows you to reuse code and/or designs multiple times without copying the artifacts. It uses the same version with variations to go from one product to the next. This is especially important for code that is being tested for security vulnerability since you may find a problem after you have made multiple products with that same code. You want to fix the code once and then have all the products use it.

Developers that take security concerns from code creation to product interfaces will be better poised to successfully become leaders in the mobile space.

Source URL (retrieved on *06/18/2013 - 2:14am*):
http://www.ecnmag.com/blogs/2010/12/security-smartphones

Links:
[1] http://www.businesswire.com/news/home/20100907006654/en/Worldwide-Converged-Mobile-Device-Market-Projections-Raised