Ryan Breuer
Article #2
Smartphone Security: Secure Software Installation on Smartphones
Article Date: May 2011

This article focuses on the security aspects of smartphones while comparing and contrasting the different methods that each carrier has implemented to keep the installation of apps secure. The article starts off by looking at recent trends of technology comparing the computers of ten years ago to the smartphones today. The improvements that have been made in technology have shifted how people interact with the web, and predicts that in the near future, smartphones may even exceed desktop systems for accessing web content. With this trend though causes a fear that mobile operating systems may become targets for malicious users to exploit.

We then move to taking a look at the top four smartphone operating systems based on their market share; these being iOS, Android, BlackBerry, and Symbian. Several features are discussed about each such as application separation, approval processes for app submission, and other aspects that make each operating system unique while still focusing on security.

After a brief introduction and history of each operating system, the article takes a much more detailed look at the security aspects that are common among them. The first of these is the process isolation mentioned earlier. This is basically limiting what each app has access to and can affect should malicious code get on there. It can be looked at as a form of damage control, which all of the mentioned operating systems implement to some point.

Next is app signing. App signing is done differently for each manufacturer, but with a similar intent, allow some form of reliance that the app is from who it says it is from. Android tends to lean towards self signing apps so that users can verify they come from a certain developer where iOS takes it much farther and requires all app be signed by them in order to be allowed on any iOS device.

All of the devices come with Read Only Memory that contains the firmware, factory restore functions for when a system gets beyond repairable, and some form of kill switches. Kill switches allow the manufacturers to stop or prevent the spread of any malicious code, policy infringing applications, or sometimes anything they want to remove. By implementing these kill switches, they can control applications even after they have been downloaded and installed on devices, which can help the non-technical users experience a worry free environment, but also limits the freedom given to them.

Going off of that, each type of phone can be categorized on a scale from Walled Garden

to Guardian to User Control. Walled Garden is the closed off system such as older phones that gave the user almost no control. Guardians control some aspects of the experience while leaving the user some choice. The User Control category focuses on systems like Android where the user is given almost complete freedom to do whatever they want, which leaves the system far more vulnerable to users who could mess something up.

Finally, there is the App Markets. Some like iOS are used to control what gets into the market and what can be spread on any iOS device, limiting the freedom that others provide, while making sure nothing harmful gets in. Others such as the Android market are used more as a central location to find apps as convenience to users more than control of what apps are submitted.

With the ever increasing technology and more information being stored on smartphones, developers will have to be extra careful to ensure the security of user's data as well as preventing malicious users from accessing it. So far, developers seem to be ahead of most of the concerns when it comes to security, but with them becoming a larger market, that may replace a large number of desktop computers, the increase of threats is also increasingly present.