Ben Collins

SE 4930

2/8/12

Article: Mobile Security Catching up? Revealing the Nuts and Bolts of the security of Mobiles Devices

Authors: Michael Becher, Felix Feiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf

Link: http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper007.pdf

Mobile Phones are an emerging platform. They have become much more sophisticated than in previous years, and now people are beginning to take the threat of mobile attacks at a more serious oberservation. The first real attacks began in March 2010, on the iOS, where an attacker was able to download the SMS (Short message system, text messages) database from users. Since several other attacks have been noticed, leaving the conclusions that a new brand of attacks against smart phones could arise.

First the article takes note in defining what a mobile phone and smart phone. Key aspects of this involves containing a mobile network operator smartcard with a connection to a mobile network. This also involves have an operating system that can be extended by a third party software. These also contain SMS and MMS systems, which differs them from a desktop computer. This are important to defining security risks of a mobile network attack.

The first idea for mobile attacks involves the creation of costs for the user. This involves either created bills for the users and other payment systems. An attack could use malware to unknowling get the user to use premium rate services (this actually was very common in message systems, I've had this happen to my phone before I had a smart phone). For me, they uses links to Facebook you could accidentally sign up for using your number, and then you would get premium text messages that cost around 2.50 a piece, which can add up.

There are four main vector classes which mobile device threats can be classified: 1) Hardware-centric attacks, which involve exploiting hardware attacks by having physical access to the phone. 2) Device-independent attacks, which involves eavesdropping on the conncetions. 3) Software centric attacks, which is considered to be the most exploitable and 4) User layer attacks, which classifies another other attach that is not of a technical nature.

What I will take away from this article is the types of security risks and the classifications of them that are out there in the mobile devices. As a mobile developer, its important to consider these things in development, especially if sensitive information will be kept on the app that is being written.