iPhone Security: 
Part 2 – iPhone App Security Model

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

My friend and colleague Adjunct Professor Richard Steinberger, CISSP, CISM from the MSIA Program< http://infoassurance.norwich.edu/ > at Norwich University< http://www.norwich.edu > continues his analysis of Apple iPhone security. Everything that follows is entirely Ric’s work with minor edits.

* * *

iPhone Apps are, with a few limited exceptions, available to iPhone owners only via Apple’s iTunes store and only if iTunes has been installed on the computer accessing the store. Users cannot, in general, download Apps from any other source, or share their Apps (even free Apps) with other iPhone owners. This distribution architecture allows Apple to vet every App that iPhone users install on their phones. In emergencies, Apple may also remotely remove or disable dangerous Apps that have been installed on iPhones.

Based on my personal observation and analysis, the main security constraints imposed by the iPhone Operating System are as follows:

- No App may access any iPhone OS files.
- No App may access any other App’s files (with a few exceptions). Any files created by an App must remain local to that App. For example, an App designed to edit Java files could only edit Java files created within that app (or downloaded to that App). Primary exceptions include: Third-party Apps may access and modify stored photos and phone contacts.
- No App may alter any system settings. For example, a precise, NTP-enabled clock may not set the iPhone’s clock.
- If an App crashes, then in theory, only that App crashes, and the OS is unaffected. In practice, a crashed App may hang a system, requiring a restart.
- An iPhone App may synchronize (sync) with a PC or Mac-based application to exchange or update the App’s data. But the syncing must be done by a wireless LAN connection and cannot be carried out using the cable that connects the iPhone to the computer; i.e., synchronization via an iTunes conduit to a PC or Mac application is not permitted.
- Apps are allowed to communicate with the Internet using the iPhone’s network connection. Thus, any data files present within an App may, in theory, be sent to an unauthorized destination without the iPhone owner’s knowledge. This transfer would be an example of an App Trojan horse program. Although such programs may escape
Apple’s initial vetting, the author knows of no cases (as of April, 2009) where such an App has actually been distributed via iTunes.

In other words, Apps are islands unto themselves. Although a rogue employee may use a mobile phone to help steal or distribute confidential information, it remains far less likely that a trustworthy iPhone owner’s use of downloadable Apps presents any major new security risk. As mentioned in the introduction, the primary risk of mobile phones remains their theft or loss. Organizations need to be prepared for the loss of confidential information when staff member phones are misplaced or stolen unless the iPhones are equipped with encryption software. In addition to using a password or personal identification number (PIN) to protect the phone itself from unauthorized access, some useful encryption and data protection Apps for the iPhone are:

- SplashID < http://www.splashdata.com/splashid/iphone/ >
- 1Password < http://agilewebsolutions.com/products/1Password >
- Verisign Identity Protection (VIP) < https://vipmobile.verisign.com/selectiphone.v >
- Jaadu VNC < http://www.jaaduvnc.com >

With appropriate precautions, corporate security managers can survive the latest wave of innovation from Apple.

* * *

Richard H. Steinberger, CISSP, CISM has over 20 years of hands-on and supervisory experience with computers and networks with special expertise in Internet and network security; security principles and products including firewalls, routers, VPNs, vulnerability assessment tools, intrusion detection systems, and hacking tools; advanced UNIX software development; and system administration. He has taught network security at University California Berkeley Engineering Extension and for several years as Adjunct Professor of Information Assurance in the MSIA Program at Norwich University. You may reach Ric by e-mail.< mailto:ricsteinberger@gmail.com >

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Copyright © 2009 Richard Steinberger & M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.