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> sent me an e-mail note recently about the interesting security model used by Apple for its mobile devices. I invited him to expand on his thoughts and am delighted to present his analysis today. Everything that follows is entirely Ric’s work with minor edits.

* * *

Perhaps the biggest security problem of mobile phones is that they are easily lost or stolen. Unless a lost/stolen phone has been protected (by its rightful owner) from unauthorized use, then anyone who finds this phone could, in theory, access it with the same rights and privileges as the original owner. But what are the security issues when the phone stays in the possession of its rightful owner? This article considers just one popular case: The Apple iPhone, although most of what applies to iPhones also applies to a related Apple product, the iTouch.

In the Summer of 2008, Apple released a new version of its iPhone (3G)<http://www.apple.com/iphone/> and a new version of the iPhone software (2.x)<http://www.apple.com/iphone/itunes.html>. Although the new software includes many commercial features, the one with the most potential security consequences is that iPhone owners can now download new applications (Apps) from Apple’s iTunes store. The iPhone became a lot more like a personal computer with a worldwide Internet connection than just a phone. iPhone users can purchase (and in many cases, acquire for free) Apps written by third party developers. By April, 2009, over one billion Apps had been downloaded, and over 25,000 Apps are available.

Apps are available in a variety of areas<http://www.apple.com/iphone/appstore/>, including reference, medical, utilities, social networking, travel, weather, news and many more. Apps (as well as music and videos) may be downloaded either directly to the iPhone over a data connection or by using Apple’s iTunes program)<http://www.apple.com/iphone/itunes.html>, installed on a PC or Mac system.

Because running third-party applications on personal computers has led to many security compromises, it’s only reasonable for IT managers to be concerned about the risks to their organization if a rogue iPhone App were to be installed on a staff member’s phone. Such installation would be a concern because: (a) many staff members connect their iPhones to the Internet using an organization’s protected wireless network, and (b) staff members could store confidential information (e.g., contacts, data files) on their iPhones. In theory, a rogue App could access or modify sensitive information or covertly send copies of it to unauthorized recipients.

How big a worry should rogue Apps be? As you will see in the next part of this two-part
overview, it’s unlikely that Apps will misbehave. The bigger concern – unaddressed in this par
of short articles – is how staff members intent on unauthorized actions could use a mobile phone
with a camera and data connection (such as an iPhone) to export confidential information using
covert channels – i.e., engage in deliberate data theft.

*Ric continues his discuss of Apple iPhone security in the next of this two-part series.*

* * *

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.