Are Apple’s Security Measures Sufficient to Protect Its Mobile Devices?

Galen A. Grimes
Department of Information Sciences and Technology
Penn State University – Greater Allegheny Campus
McKeesport, PA, USA
agrigmes@psu.edu

Abstract—Apple Computer’s iPad tablet computer has taken a commanding lead in the tablet market and history has shown that whenever a computer platform becomes dominant, it also becomes a target for malicious intruders and malware. Apple computers have long been touted as being safer from malware than their Windows counterparts, largely because of their smaller market share. This paper examines the current state of security for the iPad and mobile devices running Apple’s iPhone Operating System. Does the iPad have any vulnerabilities that need to be addressed by Apple, or is it as safe and malware-proof as some Apple devotees attest?

Keywords—iPad; iPhone; malware; mobile devices; security;

I. INTRODUCTION

Apple has long touted its seemingly invulnerability to malware on both of its platforms—Mac OS X and iPhone Operating System. The debate on the invulnerability of the Mac OS X platform has two major camps. The first faction contends that Mac OS X is based on an inherently superior software design than Microsoft Windows, and this superior design makes it more resistant to malware [1]. This group also largely dismisses the contention of the other faction, which contends that virus writers haven’t targeted Macs because Apple lacks market-share. The argument from the other camp goes that Windows dominates the worldwide PC market with Windows operating on roughly 90-95% of all personal computers and thus virus writers get more "bang for their buck" by going after the "largest fish in the ocean" [2].

If you agree with the market share argument, then Apple seemingly has created a new target for malicious hackers. The Apple iPad in its first two months took a commanding lead in the tablet computer race selling more than 2 million units [3]. Apple exceeded sales predictions in 2010 by selling more than 10 million iPads. By June of 2011 Apple had sold more than 25 million iPads worldwide making it the undeniable leader in the tablet market [4].

The iPad runs the iPhone Operating System (iPhone OS, or simply iOS) which enables it to likewise run the more than 550,000+ available iPhone applications (called “apps” for short) in addition to the more than 140,000+ apps designed specifically for the iPad with its larger screen and more powerful processor. Missing for a long time, however, from this mega-catalog of utilities, productivity apps, and games are two apps that most security experts would deem essential on any other computer system: an antivirus app and a firewall app. The first of these gaps was filled in July of 2011 when the security vendor Intego released VirusBarrier iOS for the iPhone, iPod, and iPad, making it the first anti-virus app for Apple mobile devices [5].

The VirusBarrier app is not a full-featured application like you might utilize on your desktop or laptop; but it will allow you to manually scan files in email attachments and files imported to your mobile device via DropBox. It will also allow you to manually scan files on web sites you frequent, your iDisk in your MobileMe account, and FTP or WebDAV sites.

But there is still little reason for most iOS users to worry about malware. To date, only five iOS pieces of malware have been identified ever [6] [7]. Even though Apple’s mobile products still lack a firewall app, Mac OS X since its inception has included a firewall and numerous third-party vendors have created and successfully promoted antivirus/security software for the Mac OS X platform, such as Symantec, McAfee, Sophos, and Intego even though very few verifiable pieces of malware have been identified including
a report last year about malicious spyware found in a third party screensaver [8].

Some security experts still recommend using antivirus/security software on Mac OS X to prevent Macs from becoming carriers and spreaders of malware even if they are impervious to the mostly Windows-based malware [9]. Macs are still able to forward emails containing malware without themselves becoming infected.

From a design perspective, Mac OS X and iOS are in a much better position to fend off malware than Windows. Apple maintains a much more closed and controlled hardware and software environment with Mac OS X and iOS than does Microsoft with its Windows OS. While Windows is designed to run on a seemingly endless array of hardware devices, i.e., PCs, netbooks, smartphones, etc., from an equally endless number of vendors, Mac OS X and iOS operate on a very small and tightly controlled list of hardware devices all controlled by Apple.

II. APPLE’S SECURITY DESIGN

Apple’s approach to security is as controlled as its closed hardware environment. Within Mac OS X, Apple uses a protected memory environment that its developers call “sandboxing”.

With virtually no effort on your part, Mac OS X offers a multilayered system of defenses against viruses and other malicious applications, or malware. For example, it prevents hackers from harming your programs through a technique called “sandboxing” — restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch. Other automatic security features include Library Randomization, which prevents malicious commands from finding their targets, and Execute Disable, which protects the memory in your Mac from attacks [10].

In a nutshell, Apple developers have isolated operations in the OS to prevent one program and its associated data from accessing another program and its associated data, thus providing built-in protection against malware. As secure as this model appears, Apple developers are still aware that it is not totally bulletproof and include code to protect against malware. In June of 2011 Apple developers quietly added additional anti-malware code to Snow Leopard (Mac OS X 10.6.x).

Ten months after it debuted rudimentary malware scanning in Snow Leopard, Apple this week quietly added a signature for a third piece of malware, security researchers reported today.

According to U.K.-based antivirus vendor Sophos and U.S. Mac security company Intego, Mac OS X 10.6.4, which Apple released this past Tuesday, includes an update to XProtect.

Dubbed that because the malware signatures are contained within Snow Leopard’s “XProtect.plist” file, the feature debuted in August 2009 with the launch of Mac OS X 10.6. At the time, Apple included detection for only two pieces of malware, Trojan horses named “RSPlug.a” and “I_service” by Symantec [11].

Apple developers use the same “sandboxing” memory management techniques to control program and data access inside iOS as explained in the iPhone Application Programming Guide.

For security reasons, iPhone OS restricts an application (including its preferences and data) to a unique location in the file system. This restriction is part of the security feature known as the application’s “sandbox.” The sandbox is a set of fine-grained controls limiting an application’s access to files, preferences, network resources, hardware, and so on. In iPhone OS, an application and its data reside in a secure location that no other application can access. [12].

However, the developers warn that the iOS sandbox does not provide absolute protection against attackers.

The sandbox limits the damage an attacker can cause to other applications and to the system, but it cannot prevent attacks from happening. In other words, the sandbox does not protect your application from direct attacks by malicious entities. For example, if there is an exploitable buffer overflow in your input-handling code and you fail to validate user input, an attacker might still be able to crash your program or use it to execute the attacker’s code [13].

Attacks against Apple’s Mac OS X security posture are not merely centered on whether the OS is vulnerable to malware. The hacker group that launched the attack against AT&T revealing the email addresses of more than 100,000 iPad owners has also revealed security flaws in the Safari Web browser, which is installed on both Mac OS X and iOS.

According to [Escher] Auernheimer, Goatse Security released an overflow exploit for Safari back in March. Apple patched the vulnerability for the desktop, but not for the iPad: “This bug we crafted allows the viewer of a Web page to become a proxy (behind corporate and government firewalls) for spamming, exploit payloads, password brute-force attacks, and other undesirables. The kicker is that this attack cannot be detected by any current IDS/IPS system. We released this in March, mind you, and Apple still hasn’t got around to patching this on the iPad!” Auernheimer wrote [14].
But the biggest concern about Apple’s security vulnerability involves iPhones and iPads where the users have run software to “jailbreak” the devices.

III. THE JAILBREAKING SECURITY DILEMMA

Jailbreaking is the term used to describe iPhones and iPads in which the users have run software to modify the operating system. This modification allows iPhone users in the USA and elsewhere to subscribe to a carrier other than the carriers authorized by Apple (in the USA that would include AT&T, Verizon, and Sprint) and more importantly it allows users of both devices to run “un-authorized” apps on the devices. Unauthorized apps are apps acquired outside of Apple’s online App Store. There are several hacker groups and commercial operations that provide both free and commercial jailbreaking software. Jailbreaking advocates say removing the restriction of only running Apple approved apps gives users more control over their devices.

Users who jailbreak can download apps that allow you to customize everything on the device from your homescreen images to your icons. You can also multitask by running apps in the background, tether your iPad to your PC to use it as a modem, even turn your device into a “MiFi” hotspot. Those are just the highlights, though. The jailbreak application stores (there are several, like Cydia, Icy and RockYourPhone, for example) have apps that let you do pretty much anything. Here, there really are “apps for that,” when “that” is something Apple would rather you not do [15].

Despite the so-called advantages in jailbreaking, the operation is not without its pitfalls. The normal operating system boot procedure for either the iPhone or iPad establishes a “chain of trust” among the booting components and the various apps installed on the device.

When an iPhone boots up, it walks through a "chain of trust," which is a series of signature checks among software components always done in a specific order. It begins with boot ROM, moves on to loading low-level bootloader (LLB) software (which controls general data storage and transfer between computers and digital devices, in this case flash memory), then iBoot, then the operating system kernel, and finally the OS kernel loads the user applications. As the chain of trust is executed, checks are being done for any unauthorized software [16].

This chain of trust insures that only authorized and safe programs are allowed to run on the device. In order to jailbreak an iPhone or iPad the user has to break this chain of trust.

When you jailbreak an iPhone you’re modifying, or patching, the iBoot and operating system kernel in this process, rendering them unable to do the digital signature checks that evaluate and distinguish authorized or unauthorized software [16].

The iPad was actually jailbroken using a fairly lengthy process, which involves replacing plists [property lists] on the device using replacement of files using a loosely checked backup over USB process. Carefully crafted files can be placed on the filesystem that are run and the outcome is that dyld [dynamic library loader daemon] can be encouraged to load codeless dylibs [dynamic libraries] into various process at runtime, eventually leading into a kernel exploit then the kernel can be patched in memory, and then all sorts of fun can happen, leading to the 'jailbreaking' of the device of course any Apple placed security checks (in each stage) can be patched out. The iPad hacks are considered userland [client side] exploits [17].

PandaLabs, the anti-malware laboratory of Panda Security has established that jailbreaking not only allows un-authorized apps to run on the iPhone and iPad, but jailbreaking also allows malware to run on these devices because the chain of trust created when these devices boot has been broken.

Despite the fact that Apple has made it impossible to install peripherals and software outside of those found in its own App Store, cyber-criminals have found a way to infect jailbroken iPad devices with malware. All malware designed for iPhones, such as the iPhone/Eeki. A worm that PandaLabs warned about last year, will have the same ability to infect and spread to iPad devices due to the iPad and the iPhone sharing the same operating system, known as iOS [18].

Apple engineers also carefully monitor jailbreaking software to keep abreast of the techniques that are used and if they are uncovering potential exploits in iOS.

Apple Inc has plugged a hole in the software that runs iPhones, iPads and iPod Touch music players that could allow hackers to take remote control of those devices.

The security flaw came to light nine days ago as the website www.jailbreakme.com released code that Apple customers can use to modify the iOS operating system that runs those devices through a process known as "jail breaking."

The jailbreaking code exploited a vulnerability in iOS that had not previously been disclosed. Its release gave criminal hackers a blueprint they could use to build malicious software that would exploit the vulnerability [19].

IV. IOS VULNERABILITIES VS. ANDROID OS VULNERABILITIES
Jailbreaking has become a fairly simple task. There are dozens of websites offering jailbreaking solutions ranging from free to minimally priced commercial jailbreaking and/or carrier-breaking software, not to mention the dozens of video how-to-do-its on YouTube. Some advertise jailbreaking can be completed in no more than 20 seconds. Jailbreaking software is available on Windows, Mac OS X, and Linux platforms since all of the jailbreaking software discovered so far requires a computer to connect to the device being jailbroken.

The first conclusion many iPhone and iPad users might draw is that the simple way to keep your device safe from this type of malware attack is to simply not jailbreak your mobile device.

What we are likely to see in the near future is the combination of jailbreaking software and malware—in effect, using jailbreaking software as the delivery mechanism for malware. Most likely this would come in the form of malware attacking the host PC (the computer used to sync information to the iPhone or iPad). This is a likely scenario considering the vast amount of malware in the Windows environment and considering that a significant number of Mac and Linux users still do not utilize antivirus software in the mistaken belief that their computers are immune to malware [20].

It is also conceivable that a malicious hacker could purposely and surreptitiously include/infect jailbreaking code with malware and then simply distribute the software as a new jailbreaking application. Once you connect your iPhone or iPad to your PC and run a jailbreaking application there is no way to determine what has been done to your device until it is too late. Right now iPhone and iPad users who jailbreak their devices are blindly trusting the developers from whom they acquired their jailbreaking application.

JailbreakMe.com 3.0 exploits a vulnerability in the PDF reader. The iOS Safari browser downloads a PDF file that triggers a vulnerability in how the built-in PDF reader handles a certain font type. "This is what installs the actual jailbreak," explains Stephan Chenette, manager of security research at Websense, a content security company.

So why is it so dangerous? An attacker can reverse engineer JailbreakMe.com 3.0 to silently install malicious code through the browser or email attachment. "Then the attacker could gain full control of the iPhone, iPad or other iOS device and install everything from a keylogger to a full-blown bot," Chenette says. "This isn't just limited to iPhones; iPad users need to be on the lookout, too" [21].

There is no evidence yet that any jailbreaking software has been infected with malware, and from all anecdotal indications most users of jailbreaking software seemed very pleased with both the ease of use of the software and the results of jailbreaking their devices. There is also no reliable indicator of what percentage of iPhone or iPad users have jailbroken their devices. There are some indications that a high percentage of jailbroken devices are overseas, primarily in markets where Apple is not yet officially selling iPhones and iPads and users are acquiring the devices from sources such as eBay and Craigslist.

While iOS by design does attempt to address many of the security concerns around malware, little has been said in the mainstream media about the potential security vulnerabilities inherent in the Android OS because of its open source design, especially considering the size of the Android OS market share.

...In May this year we've seen the Man in the Mobile (MitMo) malware - which has previously attacked Symbian, Blackberry, and Windows phones - being ported to Android as well," he adds.

And the Apple iOS platform notes Boodai, is also not as safe as people think, as a jailbroken iOS device does not enforce access control - as seen on the iTunes app portal - and allows any application to do whatever it likes on the device.

Unfortunately, he says, many users jailbreak their devices as they want to run all sorts of applications that are not on the iTunes app store.

"But what's more unfortunate is that vulnerabilities in iOS could allow malicious websites to jailbreak a device and infect it with malware without the user's consent or knowledge", he says [22].

Google does not subject Android apps submitted to its market distribution site to the same rigors as does Apple for apps submitted to the iTunes App Store, and Google has on several occasions had to remove malware-infected apps from its distribution site.

Google has removed nearly two dozen malware-infected apps from its official Android Market in the last several days, a security company said Sunday.

So far this year, Google has yanked more than 100 malicious Android apps from its distribution channel [23].

...any app on affected devices that requests a single android.permission.INTERNET (which is
normal for any app that connects to the web or shows ads) can get its hands on:

- the list of user accounts, including email addresses and sync status for each
- last known network and GPS locations and a limited previous history of locations
- phone numbers from the phone log
- SMS data, including phone numbers and encoded text (not sure yet if it's possible to decode it, but very likely)
- system logs (both kernel/dmesg and app/logcat), which includes everything your running apps do and is likely to include email addresses, phone numbers, and other private info [24].

But Google may be facing a much more difficult task in its attempt to shore up its vulnerable OS.

A simple conclusion to be drawn is that Android suffers from security flaws. It appears that a lack of trusted digital signatures for apps in Android is a problem. Use of an insecure Java-based virtual machine to execute apps may also be an issue. In Android, fixing security issues is problematic because a different version for each carrier, manufacturer and model is required. Further, many Android devices use insecure and old versions of the operating system. It appears Android may become more vulnerable as the sophistication of tools that allow for automatic repackaging of legitimate apps to add malware, allow malware to hide in advertisements, and allow botnets to steal data increases [25].

V. CONCLUSION

With the increased popularity of smartphones due in large part to the increased functionality and the proliferation of more sophisticated apps, especially financial apps, the next wave of malware attacks is predicted to favor the same target paradigm as have malware developers who have spent the last two decades targeting Windows-based computers—you go where you are likely to get the most bang for your buck. And in the immediate future that would appear to be the Android platform since Android in all its flavors commands 47 percent of the smartphone market [28], and because Android seems to be the most vulnerable, and for now continues to divert this unwanted attention away from Apple’s iOS.

But Apple can’t expect Google and Android to continue to divert attention away from its OS forever. Because of the increased use of smartphones and other mobile devices in the corporate setting, and because of the increased development and use of more sophisticated financial apps, Apple is certainly moving its OS into the crosshairs.

Are financial apps on mobile devices destined to be the next target of malicious hackers?

It was found that Zues [sic], the notorious malicious code that steals online banking information, also operates in various mobile environments. The malicious code called Zitmo (Zues [sic] In The Mobile) was first discovered in Symbian and Blackberry, and is recently found in the Android Platform. Zitmo in Android has disguised itself as an online banking security product. It taps text transmission history to penetrate a two-factor authentication system that requires two factors, including OTP (One Time Password) and text messaging, for authentication [26].

Predictions of attacks on smartphones and mobile devices don’t just include attacks seeking your financial information. These attacks can also take the form of malware that perform direct billing on your wireless account. These types of attacks are predicted to explode in number.

Malicious applications that perform direct billing were the bulk of Android based threats in 2011. This type of malware exploits the fact that the smartphone OS includes calling and texting functions by using premium call settings. When the device is infected with this type of malware, it sends text messages to a certain number that generates a premium fee to the sender without permission from the user. Android-Trojan/Pavelsms is the most recently malicious code discovered in a scam app, which is also known as the ‘ruFraud’ [26].

Fortunately, iOS is not susceptible to these types of attacks because it requires user confirmation for premium-rate SMS messages. But this does not mean iOS is immune to other types of direct billing and financial attacks. According to Felt et al., “we think that credential theft, credit card theft via NFC [Near Field Communication], and advertising click fraud are the most likely to be targeted by future malware authors” [6].

Attacking through fraudulent apps is also expected to see an increase in the future. Apple for now seems to be avoiding many of the pitfalls that have befallen Android, and to a lesser degree Symbion, by including in its app approval process human review before an app is included in the App Store.

And finally, there is the threat of root exploits, the whole impetus of the jailbreak phenomenon. While a significant number of users want to customize their smartphones beyond what the manufacturers authorize by utilizing root exploits, so too do malware authors have an incentive to find and utilize these same root exploits. Unfortunately, it is not terribly difficult for malware authors to discover smartphone root
exploits since many are published by the homebrew community in an attempt to help owners of smartphones in their efforts to customize their devices.

Rooting of Android OS or 'jail breaking' the iPhone generally exploits applications' vulnerabilities. These methods enable the users to get 'super user' permission, allowing for full control of the kernel of the operating system. While super user permission allows users to control many restricted functions of the smartphone, this mighty authority can bring serious security threats when in the wrong hands. For instance, the attackers with super user permission can delete the system to disable all functions of the smartphone, or install undeletable malicious applications. The possibility of distribution of kernel-attacking technology could sharply increase as the number of mobile malware is increasing [26].

One recommendation that could go a long way in heading off root exploits would be for manufacturers, including Apple, to support smartphone customization instead of fighting it. This way they could control the customization that some users insist on performing and not allow it to circumvent their security mechanisms.

REFERENCES


[17] Pytey [Member of the iPhone Dev Team], Email, June 24, 2010.


others-exposes-phone-numbers-gps-sms-emails-addresses-much-more/


JAILBREAKING WEBSITES

SpiritJB—http://spiritjb.com
IH8Sn0w— http://ih8sn0w.com/index.php/welcome.sn0w
Redmond Pie— http://www.redmondpie.com/pwnagetool-4.0-jailbreak-ios-4-iphone-3g-3gs/
Appli iPhone Review—
http://www.appleiphonereview.com/iphone-tutorials/how-to-jailbreak-unlock-iphone-2g-v-3-0/
BlogsdNA— http://www.blogsdna.com/3718/how-to-jailbreak-iphone-3g-30-with-quickpwn-on-windows-mac.htm

iPhone Hacks—
JailBreakMe.com— http://www.jailbreakme.com