the Availability Digest

www.availabilitydigest.com

Malicious Apple Chargers

August 2013

Researchers at the Georgia Institute of Technology have discovered an unlikely back door into Apple devices. Billy Lau, Yeongjin Jang, and Chengyu Song have demonstrated that they can easily build an Apple device charger that can infect an iPhone or an iPad. Known for its high level of security and vetting of apps, Apple devices are seldom compromised by hackers (not so for Android devices). Apple has quickly responded with an upgrade to close the security flaw.

The key to compromising an iPhone or an iPad is the fact that such devices are charged through a USB port. The USB port supplies not only a provision for charging the internal batteries of the device but also provides a gateway to the device's operating system and applications. This is, of course, the primary purpose of the USB port – to provide (presumably secure) access to the iOS internals for external devices.

The researchers used the USB portal into the devices to infect them within sixty seconds of being plugged in. Fortunately, there are no known instances of this hack being used in the real world – yet.

The Disclosure

Georgia Tech's Information Security Center notified Apple in June, 2013, so that Apple could patch its operating system before the researchers went public with their discovery. The researchers then described their technique and demonstrated a working proof of concept at the Black Hat USA 2013 security conference held at Caesar's Palace in Las Vegas from July 27 through August 1, 2013. They plugged an iPhone into their malicious charger and within a minute showed that a Facebook application in the iPhone had been replaced with a malicious app.

Their talk was entitled "Mactans: Injecting Malware into iOS Devices via Malicious Chargers." The abstract for their talk read as follows:

> "Apple iOS devices are considered by many to be more secure than other mobile offerings. In evaluating this belief, we investigated the extent to which security threats were considered when performing everyday activities such as charging a device. The results were alarming: despite the plethora of defense mechanisms in iOS, we successfully injected arbitrary software into current-generation Apple devices running the latest operating system (OS) software. All users are affected, as our approach requires neither a jailbroken device nor user interaction.
>
> "In this presentation, we demonstrate how an iOS device can be compromised within one minute of being plugged into a malicious charger. We first examine Apple's existing security mechanisms to protect against arbitrary software installation, then describe how USB capabilities can be leveraged to

bypass these defense mechanisms. To ensure persistence of the resulting infection, we show how an attacker can hide their software in the same way Apple hides its own built-in applications.

To demonstrate practical application of these vulnerabilities, we built a proof of concept malicious charger, called Mactans, using a BeagleBoard. This hardware was selected to demonstrate the ease with which innocent-looking, malicious USB chargers can be constructed. While Mactans was built with limited amount of time and a small budget, we also briefly consider what more motivated, well-funded adversaries could accomplish. Finally, we recommend ways in which users can protect themselves and suggest security features Apple could implement to make the attacks we describe substantially more difficult to pull off."

The Malicious Charger

The researchers built their charger using a small $45 BeagleBoard Linux computer from Texas Instruments. They named their charger Mactans, which is the scientific name for the Black Widow spider.

Though the BeagleBoard is quite small – about the size of a credit card, it is much too large to fit into an Apple charger casing. It is unlikely (though not impossible) to be scaled down to the size of an Apple iPhone or iPad charger any time soon.

The Attack Methodology

The researchers took advantage of Apple's developer model. The model allows an enrolled developer to register a device's Unique Device Identifier (UDI) to prove that the device is his. The UDI is then used on an Apple website to take advantage of an Apple uploading tool that allows the developer to download an app under development so that he can test his software on an iOS device.

At this point, the developer can install any third-party app on that iPhone or iPad, whether or not the app has been approved by Apple.

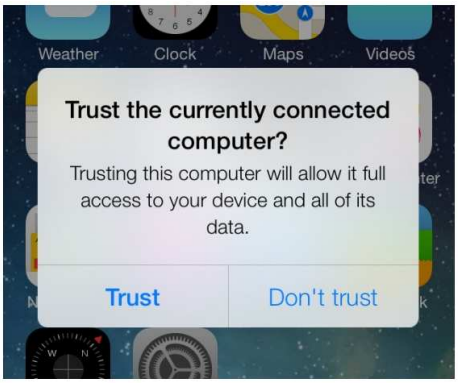
The hack proceeds as follows. The hacker first registers with Apple to become a developer. When plugged into the iDevice, the Mactans malicious charger interrogates the iDevice via the USB port to obtain its UDI. Mactans then registers the device as the developer's test device in seconds. At this point, Mactans, acting as the developer, can install any malware it wants.

In the demo, the researchers loaded a fake Facebook app and replaced the real Facebook app with the fake one. In this way, the iOS had no idea that a malicious app had been installed. The fake Facebook app could grab screenshots, simulate button touches, and send data to a remote server.

The attack only works on unlocked devices. So long as devices are locked, the malicious charger can not get access to it. As a hacking tool, it also has limited use since it isn't scalable. It works only on a one-to-one basis as it can infect only the iDevice to which it is attached.

Apple's Security Fix

As soon as the researchers discovered the security flaw, they notified Apple. Apple added a security fix to iOS 7 that warns the user that it is attached to a different computer (after all, that is what Mactans is). The prompt displays the following message and asks for the user's permission to attach to the computer:



Untrusted devices are given no access to the internals of the iOS device.

Apple has thanked the researchers for their important input and has stated that the issue has been addressed in iOS 7. iOS 7 is currently in Beta testing as of this writing, and Apple has not committed to making the change available in any of its earlier operating system versions.

Summary

Mactans is an interesting means to infect a device. We don't usually worry about the access that a charger might have to our iPhones or iPads. Should we watch out for this on Android devices?

In any event, Mactans does not seem to present an immediate danger. It is unlikely to be packaged to look like a standard iDevice charger, and is a threat only to the one iDevice it is plugged into and only if that device is unlocked.

This is not the first problem Apple has faced with its chargers. Apple is plagued with cheap fake versions of its chargers. In July, 2013, a Chinese woman was electrocuted by a fake charger. The following week, a man was shocked into a coma by a fake charger. Apple has now offered to buy back any iPhone, iPad, or iPod charger not made by Apple and to replace it with an authentic Apple charger at half price.

Acknowledgements

Material for this article was taken from the following sources:

Mactans: Injecting Malware into iOS Devices via Malicious Chargers, *Black Hat USA 2013 Paper Abstract*.
Any iOS device can be hacked within one minute with modified charger, say researchers, *The Verge*; June 3.
Apple will keep fake chargers from hacking your iPhone with iOS 7, *The Verge*; July 31, 2013.
Apple update to tackle charger hack attack, *BBC*; August 1, 2013.
Apple: iOS 7 fixed the nefarious charger hack, *TUAW – The Unofficial Apple Weblog*; August 1, 2013.
Apple finally Fixed the Bug That Let Fake Chargers Hack Your iPhone, *Gizmodo*; August 1, 2013.
Apple fixed Malicious Charger Hack in iOS , *iPhone Hacks*; August 1, 2013.
iPhone Hacked in Under 60 Seconds Using Malicious Charger, *Slashdot*; August 1, 2013.
Apple Fixes Charger-Based Hack in iOS 7 Beta 4, *AddAdvice*; August 1, 2013.
Apple's 'walled garden' cracked by hacked charger, *CSO Online*; August 2, 2013.
Apple's iPhone charger take-back program is genius PR – and it may even boost the bottom line, *Quartz*; August 7, 2013.