# Apple says it has patch for remote hack attack

August 9 2010, By Byron Acohido, USA Today

Apple is quietly wrestling with a security conundrum. How the company handles it could dictate the pace at which cybercriminals accelerate attacks on iPhones and iPads.

Apple is hustling to issue a patch for a milestone security flaw that makes it possible to remotely hack - or jailbreak - iOS, the operating system for iPhones, iPads and iPod Touch.

The patch is completed, Apple spokeswoman Natalie Kerris said in an interview. But Kerris said on Friday that she was not able to give a time frame for its public release.

Jailbreaking refers to hacking iOS to download Web apps not approved by Apple. This used to be difficult. This spring, a website came along called JailbreakMe.com that made it trivial to jailbreak your own iPhone or iPad. Last week, a technique for remote jailbreaking appeared on the site. It's now possible to access the operating system of an iPhone or iPad owned by someone else.

An attacker would get "fairly complete control of affected devices," says Michael Price, an operations manager for McAfee Labs. No such attacks are known to have happened yet, he says.

For the moment, the most visible concern for Apple has been pranksters going into Apple and Best Buy retail stores and jailbreaking display models, according to tech blog Engadget. Yet, the security and privacy issues are serious.

Security experts expect the pattern that has come to dominate the PC world to begin to permeate smartphones. Bad guys continually flush out new security flaws in PCs, then tap into them to launch malicious attacks. Good guys, meanwhile, scramble to patch and block.

Now, cybercriminals are rapidly adapting PC hacking techniques to all smartphone platforms, including Symbian, Google Android, Windows Mobile, RIM BlackBerry and Apple iOS.

"It's a brand new game with new rules," says Dror Shalev, chief technology officer of DroidSecurity, which supplies protection for Google Android phones. "We're seeing rapid growth in threats as a side effect of the mobile Web app revolution."

IPhones, in particular, have become a pop culture icon in the U.S., and now the iPad has grabbed the spotlight. "The more popular these devices become, the more likely they are to get the attention of attackers," says Joshua Talbot, intelligence manager at Symantec Security Response.

Apple's problem is singular. The company has made a big deal about hiding technical details of iOS, allowing only approved Web apps to tie in. This tight control initially made it easier to keep iOS secure. But now Apple may have to share iOS coding with anti-virus firms, says Sorin Mustaca, development manager for anti-virus firm Avira.

Windows, Google, Nokia and RIM share such coding to help anti-virus firms develop protections. "Apple does not allow this, making it challenging for anti-virus vendors to create third-party protection for iPhones and iPads," Mustaca says.

Pressure is building. Mikko Hyponnen, senior researcher at anti-virus firm F-Secure, says hackers are likely working on a worm to take control of jailbroken iPads and iPhones. "My guess is we'll see it within a week," Hyponnen says. "There's very little users can do to protect themselves beforehand."

Apple is aware of the threat, but not saying much publicly. "We'll do everything we can to make sure this is not an issue for our customers," Kerris says.

Apple must coordinate patching with some 15 phone companies worldwide, says John Hering, CEO of mobile security firm Lookout. And iPad and iPhone users likely will have to manually install the patch via iTunes. "We're in a cat-and-mouse game with openness and security at odds, and consumers stuck right in the middle," Hering says.

Visit USA Today on the Internet at www.usatoday.com/
Distributed by McClatchy-Tribune Information Services.