How all your iPhone apps could be hacked at once

By David Goldman @CNNMoneyTech July 27, 2012: 5:15 AM ET

Almost every app on the iPhone relies heavily on Apple's built-in security.

LAS VEGAS (CNNMoney) -- The iPhone's baked-in security has improved dramatically over the past few years, which is great for Apple fans.

In a weird way, it's good for hackers too.

With the "bring your own device" phenomenon in full-swing, Apple (AAPL, Fortune 500) has been successful at getting its iPhones and iPads into the hands of Fortune 500 companies and even many government agencies, including the White House and the U.S. military. To make those sales, Apple had to update its iOS mobile operating system with some of the industry's most robust security features.

That had a nasty unintended consequence: Many app developers no longer put their own safeguards in place, relying instead almost exclusively on Apple to ensure the security of their applications.

With thousands of apps in the iTunes App store all featuring the same exact security features, one single vulnerability could have a domino effect.

"Security is now an afterthought for many app developers," said Jonathan Zdziarski, senior forensic scientist at viaForensics, in a presentation at the Black Hat cybersecurity conference in Las Vegas on Thursday. "That means if you hack one, you can hack them all."

Apple declined to comment.

The tech giant made its first official appearance at Black Hat this year with a session on iOS's security features, but the dry presentation was little more than a public reading of a white paper Apple recently released. Presenter Dallas De Atley, Apple's platform security team manager, took no questions after his talk and quickly escaped out a side door.

A few rooms away, Zdziarski simultaneously delivered his workshop on "The Dark Art of iOS Application Hacking."

The scenarios Zdziarski outlined are scary, but they're also far-fetched.

To hack all the apps on your phone, a hacker would need to: 1) steal your iPhone, which isn't so hard, and 2) discover and exploit an iOS vulnerability before Apple does. That's proven to be very hard. It has happened before -- most notably when serial Apple hacker Charlie Miller found a way to sneak a rogue app into Apple's fiercely guarded iTunes store. (When he publicized the hack, Apple yanked his developer license.)

Still, so-called "zero day exploits" on iOS have been extremely rare.

Related story: Your eyeballs are hackers' next target

"This isn't Chicken Little and the sky is falling," Zdziarski told CNNMoney. "But the message is if you don't add your own security to your app, you're highly susceptible."

To illustrate, Zdziarski live-demonstrated some of the vulnerabilities of a few popular iOS apps that don't add much more security above Apple's baked-in protections.

A bug in PayPal's app, for instance, allows a hacker to place malicious code in a stolen iPhone and get all the log-in information that a user enters. It's unlikely. The hacker would need about 20 minutes with the iPhone to do it before handing the phone back to the owner. But the point is it's possible -- and it shouldn't be.

PayPal, a subsidiary of eBay (EBAY, Fortune 500), said it is investigating the issue.

"The security of our users is a top priority for PayPal," the company said in a statement. "One of the benefits of using PayPal on a mobile device is that a user's financial information is stored in the cloud and not on his or her device. Therefore, even if a device is compromised a user's financial information is inaccessible."

One vulnerable spot is Apple's lack of password confirmations any time a user returns to an app they've previously logged into. In one demo, Zdziarski tweaked an app's code and entered,

"userIsLogged: 1." That "1" means "true" in this case, and the app was tricked into thinking the user had been properly identified.

Zdziarski's end goal wasn't to call out Apple, PayPal or any company in particular, he said. Rather, it was simply to warn developers not to be lazy when dealing with security in their iPhone apps.

"Apple has good security," Zdziarski said. "Just don't rely entirely upon it."

-- *CNNMoney tech editor Stacy Cowley contributed reporting to this article.*