

INSIGHT ON TECHNOLOGY

THINK YOUR SMARTPHONE IS SECURE?



So far, there have been few publicly identified, large-scale, smartphone security breaches, but just because it hasn't happened yet doesn't mean it won't. With about 164 million smartphone users in the United States, 167 million people accessing the Internet from mobile devices, business firms increasingly switching their employees to the mobile platform, and consumers using their phones for financial transactions and even paying bills, the size and richness of the smartphone target for hackers is growing.

Have you ever purchased anti-virus software for your smartphone? Probably not. Many users believe their smartphones are unlikely to be hacked because Apple and Google are protecting them from malware, and that Verizon and AT&T can keep the cell phone network secure just as they do the land-line phone system. Telephone systems are "closed" and therefore not subject to the kinds of attacks that occur on the open Internet.

Hackers can do to a smartphone just about anything they can do to any Internet device: request malicious files without user intervention, delete files, transmit files, install programs running in the background that can monitor user actions, and potentially convert the smartphone into a robot that can be used in a botnet to send e-mail and text messages to anyone.

Apps are one avenue for potential security breaches. Apple, Google, and RIM (BlackBerry) now offer over 2.5 million apps collectively. Apple claims that it examines each and every app to ensure that it plays by Apple's iTunes rules, but risks remain. Most of the known cases that occurred thus far have involved jailbroken phones. The first iPhone app confirmed to have embedded malware made it past Apple into the

iTunes store in July 2012. However, security company Kaspersky expects the iPhone to face an onslaught of malware over the course of the next year. Apple iTunes app rules make some user information available to all apps by default, including the user's GPS position and name. However, a rogue app could easily do much more. Nicolas Seriot, a Swiss researcher, built a test app called SpyPhone that was capable of tracking users and all their activities, then transmitting this data to remote servers, all without user knowledge. The app harvested geolocation data, passwords, address book entries, and e-mail account information. Apple removed the app once it was identified. That this proof-of-concept app was accepted by the iTunes staff of reviewers suggests Apple cannot effectively review new apps prior to their use. Thousands of apps arrive each week. Also, Apple's 'walled garden' approach means that only Apple is truly qualified to defend iOS devices from attacks. Until it changes this policy, third parties won't be able to develop services to protect Apple devices as they may be able to with Android.

The amount of malware on the Android platform has skyrocketed over the past year. According to Cisco, 99% of all mobile malware in 2013 targeted Android devices. In part this is due to the fact that security on that platform is much less under the control of Google because it employs an "open" app model compared to Apple's "walled garden" approach. In addition, in the past, Google did not review Android apps, instead relying on user input and technical hurdles to limit malware. However, in 2013, in response to the growing malware problem, Google launched a universal app-scanning system that instantly checks each app for malicious code at the device level.

Android apps run in a “sandbox,” where they cannot affect one another or manipulate device features without user permission. Android apps can use any personal information found on a Droid phone but they must also inform the user what each app is capable of doing, and what personal data it requires. Google removes any apps that break its rules against malicious activity. One problem: users may not pay attention to permission requests and simply click “Yes” when asked to grant permissions. Apple’s iPhone does not inform users what information apps are using, but does restrict the information that can be collected by any app.

Google can perform a remote wipe of offending apps from all Droid phones without user intervention. This is a wonderful capability, but is itself a security threat if hackers gain access to the remote wipe capability at Google. In one incident, Google pulled down dozens of mobile banking apps made by a developer called 09Droid. The apps claimed to give users access to their accounts at many banks throughout the world. In fact, the apps were unable to connect users to any bank, and were removed before they could do much harm. Google does take preventive steps to reduce malware apps such as vetting the backgrounds of developers, and requiring developers to register with its Google Wallet payment service (both to encourage users to pay for apps using their service as well as to force developers to reveal their identities and financial information).

Beyond the threat of rogue apps, smartphones of all stripes are susceptible to browser-based malware that takes advantage of

vulnerabilities in all browsers. In addition, most smartphones, including the iPhone, permit the manufacturers to remotely download configuration files to update operating systems and security protections. Unfortunately, flaws in the public key encryption procedures that permit remote server access to iPhones have been discovered, raising further questions about the security of such operations. Attackers have also developed methods of hijacking phones using weaknesses in SIM cards. There are at least 500 million vulnerable SIM cards in use today, and the defects allow hackers to obtain the encryption key that guards users’ personal information, granting them nearly complete access over the phone in the process.

In 2013, internal NSA documents indicated that the law enforcement agency had developed the capability to tap into sensitive personal data held on all major smartphone devices, even the BlackBerry mail system, which is considered the most secure of any smartphone. In 2011, the NSA was also granted the ability to conduct warrantless searches of American communications in a way that had previously been reserved only for foreigners. While the NSA had devoted entire teams to individual smartphone operating systems in order to make this breakthrough, their success is proof-of-concept for other more malicious organizations to develop similar capabilities.

Suddenly, our smartphones and tablets don’t seem quite as safe anymore. Some commentators dismiss these concerns as more hype than reality. But reality is catching up with the hype.

SOURCES: “Cisco 2014 Annual Security Report,” 2014; “NSA Secretly Broke Smartphone Security,” by Cory Doctorow, BoingBoing.com, September 8, 2013; “Obama Administration Had Restrictions on NSA Reversed in 2011,” by Ellen Nakashima, September 7, 2013; “How Google Just Quietly Made Your Android Phone More Secure,” by JR Raphael, *Computerworld*, July 26, 2013; “Crypto Flaw Makes Millions of Smartphone Susceptible to Hijacking,” by Dan Goodin, *ArsTechnica.com*, July 22, 2013; “Android Will Account for 58% of Smartphone App Downloads in 2013, with iOS Commanding a Market Share of 75% in Tablet Apps,” ABI Research, March 4, 2013; “Smartphone Cyberattacks to Grow This Year,” by David Goldman, *money.cnn.com*, January 8, 2013; “iPhone Malware: Spam App ‘Find and Call’ Invades App Store,” by Zach Epstein, *BGR.com*, July 5, 2012; “iPhone Malware: Kaspersky Expects Apple’s iOS to be Under Attack by Next Year,” by Sara Gates, *Huffington Post*, May 15, 2012; “Android, Apple Face Growing Cyberattacks,” by Byron Acohido, *USA Today*, June 3, 2011; “Security to Ward Off Crime on Phones,” by Riva Richmond, *New York Times*, February 23, 2011; “AT&T Plans Smartphone Security Service for 2012,” “Smartphone Security Follies: A Brief History,” by Brad Reed, *Network World*, April 18, 2011.