Your smartphone: a new frontier for hackers

August 8 2011, By JORDAN ROBERTSON , AP Technology Writer

In this Jan. 5, 2011 file photo, a person operates their iPhone in New York. Security experts say attacks on smartphones are growing fast — and attackers are becoming smarter about developing new techniques. (AP Photo/Frank Franklin II, File)

(AP) -- Hackers are out to stymie your smartphone. Last week, security researchers uncovered yet another strain of malicious software aimed at smartphones that run Google's popular Android operating system. The application not only logs details about incoming and outgoing phone calls, it also records those calls.

That came a month after researchers discovered a security hole in Apple

Inc.'s iPhones, which prompted the German government to warn Apple about the urgency of the threat.

Security experts say attacks on smartphones are growing fast - and attackers are becoming smarter about developing new techniques.

"We're in the experimental stage of mobile malware where the bad guys are starting to develop their business models," said Kevin Mahaffey, co-founder of Lookout Inc., a San Francisco-based maker of mobile security software.

Wrong-doers have infected PCs with malicious software, or malware, for decades. Now, they are fast moving to smartphones as the devices become a vital part of everyday life.

Some 38 percent of American adults now own an iPhone, BlackBerry or other mobile phone that runs the Android, Windows or WebOS operating systems, according to data from Nielsen. That's up from just 6 percent who owned a smartphone in 2007 when the iPhone was released and catalyzed the industry. The smartphone's usefulness, allowing people to organize their digital lives with one device, is also its allure to criminals.

All at once, smartphones have become wallets, email lockboxes, photo albums and Rolodexes. And because owners are directly billed for services bought with smartphones, they open up new angles for financial attacks. The worst programs cause a phone to rack up unwanted service charges, record calls, intercept text messages and even dump emails, photos and other private content directly onto criminals' servers.

Evidence of this hacker invasion is starting to emerge.

- Lookout says it now detects thousands of attempted infections each day

on mobile phones running its security software. In January, there were just a few hundred detections a day. The number of detections is nearly doubling every few months. As many as 1 million people were hit by mobile malware in the first half of 2011.

- Google Inc. has removed about 100 malicious applications from its Android Market app store. One particularly harmful app was downloaded more than 260,000 times before it was removed. Android is the world's most popular smartphone operating software with more than 135 million users worldwide.

- Symantec Corp., the world's biggest security software maker, is also seeing a jump. Last year, the company identified just five examples of malware unique to Android. So far this year, it's seen 19. Of course, that number pales compared with the hundreds of thousands of new strains targeting PCs every year, but experts say it's only a matter of time before criminals catch up.

"Bad guys go where the money is," said Charlie Miller, principal research consultant with the Accuvant Inc. security firm, and a prominent hacker of mobile devices. "As more and more people use phones and keep data on phones, and PCs aren't as relevant, the bad guys are going to follow that. The bad guys are smart. They know when it makes sense to switch."

When it comes to security, smartphones share a problem with PCs: Infections are typically the responsibility of the user to fix, if the problem is discovered at all.

The emergence in early July of a previously unknown security hole in Apple Inc.'s iPhones and iPads cast a spotlight on mobile security. Users downloaded a program that allowed them to run unauthorized programs on their devices. But the program could also be used to help criminals co-

opt iPhones. Apple has since issued a fix.

It was the second time this year that the iPhone's security was called into question. In April the company changed its handling of location data after a privacy outcry that landed an executive in front of Congress. Researchers had discovered that iPhones stored the data for a year or more in unencrypted form, making them vulnerable to hacking. Apple CEO Steve Jobs emerged from medical leave to personally address the issue.

The iPhone gets outsize attention because it basically invented the consumer smartphone industry when it was introduced in 2007. But Apple doesn't license its software to other phone manufacturers. Google gives Android to phone makers for free. So, Android phones are growing faster. As a result, Google's Android Market is a crucial pathway for hacking attacks. The app store is a lightly curated online bazaar for applications that, unlike Apple's App Store, doesn't require that developers submit their programs for pre-approval.

Lookout says it has seen more unique strains of Android malware in the past month than it did in all of last year. One strain seen earlier this year, called DroidDream, was downloaded more than 260,000 times before Google removed it, though additional variants keep appearing.

Lookout says about 100 apps have been removed from the Android Market so far, a figure Google didn't dispute.

Malicious applications often masquerade as legitimate ones, such as games, calculators or pornographic photos and videos. They can appear in advertising links inside other applications. Their moneymaking schemes include new approaches that are impossible on PCs.

One recent malicious app secretly subscribed victims up to a service that

sends quizzes via text message. The pay service was charged to the victims' phone bills, which is presumably how the criminals got paid. They may have created the service or been hired by the creator to sign people up. Since malware can intercept text messages, it's likely the victims never saw the messages - just the charges.

A different piece of malware logs a person's incoming text messages and replies to them with spam and malicious links. Most mobile malware, however, keep their intentions hidden. Some apps set up a connection between the phone and a server under a criminal's control, which is used to send instructions.

Google points out that Android security features are designed to limit the interaction between applications and a user's data, and developers can be blocked. Users also are guilty of blithely click through warnings about what personal information an application will access.

Malicious programs for the iPhone have been rare. In large part, that's because Apple requires that it examine each application before it goes online. Still, the recent security incidents underline the threat even to the most seemingly secure devices.

A pair of computer worms targeting the iPhone appeared in 2009. Both affected only iPhones that were modified, or "jailbroken," to run unauthorized programs.

And Apple has dealt with legitimate applications that overreached and collected more personal data than they should have, which led to the Cupertino, Calif.-based company demanding changes.

"Apple takes security very seriously," spokeswoman Natalie Kerris said in July. "We have a very thorough approval process and review every app. We also check the identities of every developer and if we ever find

anything malicious, the developer will be removed from the iPhone Developer Program and their apps can be removed from the App Store."

A criminal doesn't even need to tailor his attacks to a mobile phone. Standard email-based "phishing" attacks - tricking people into visiting sites that look legitimate - work well on mobile users. In fact, mobile users can be more susceptible to phishing attacks than PC users.

The small screens make it hard to see the full Internet address of a site you're visiting, and websites and mobile applications working in tandem train users to perform the risky behavior of entering passwords after following links, new research from the University of California at Berkeley has found.

The study found that the links within applications could be convincingly imitated, according to the authors, Adrienne Porter Felt, a Ph.D. student, and David Wagner, a computer science professor.

They found that "attackers can spoof legitimate applications with high accuracy, suggesting that the risk of phishing attacks on mobile platforms is greater than has previously been appreciated."

A separate study released earlier this year by Trusteer, a Boston-based software and services firm focused on banking security, found that mobile users who visit phishing sites are three times more likely to submit their usernames and passwords than desktop PC users.

Mobile users are "always on" and respond to emails faster, in the first few hours before phishing sites are taken down, and email formats make it hard to tell who's sending a message, Trusteer found.

Still, mobile users have an inherent advantage over PC users: Mobile software is being written with the benefit of decades of perspective on

the flaws that have made PCs insecure. But smartphone demand is exploding, with market research firm IDC predicting that some 472 million smartphones will be shipped this year, compared with 362 million PCs. As a result, the design deterrents aren't likely to be enough to keep crooks away from the trough.

"It's going to be a problem," Miller said. "Everywhere people have gone, bad guys have followed."