Smart phones easily invaded, researchers find

July 9 2010, By David Sarno

Security researchers Nick DePetrillo and Don Bailey have discovered a seven-digit numerical code that can unlock all kinds of secrets about you. It's your phone number.

Using relatively simple techniques, this duo can use your cell phone number to figure out your name, where you live and work, where you travel and when you sleep. They could even listen to your voice messages and personal phone calls -- if they wanted to.

"It's really interesting to watch a phone number turn into a person's life," DePetrillo said.

"Everyone's taught to keep their Social Security number a secret," Bailey said. "But the phone number seems just as dangerous, if not more so."

The world has come a long distance from old-style telephones, which were little more than a speaker, a bell and a microphone connected to a wire.

But as smart phones become more powerful and widely used, they also become busy hubs for data, packed with a user's digital Rolodex, e-mails and credit card details. Most phones are also fitted with a global positioning device that beams its location far and wide.

Taken together, this trove of personal information is valuable to both legitimate commercial companies and unwelcome intruders.

In the last several years, tens of millions of consumers have turned in their older-model cell phones in exchange for high-tech, computer-like handsets such as Apple Inc.'s iPhone, Google Inc.'s Android phones and Research in Motion Ltd.'s line of BlackBerry devices.

Used by about 21 percent of mobile phone customers, smart phones are quickly gaining ground on the previous generation of simpler flip phones, and by 2011 they are likely to become the standard for most consumers, according to Nielsen Co.

DePetrillo and Bailey are part of a busy community of security researchers -- some of whom are known as "white hat" hackers -- investigating and exposing the many security holes that have yet to be plugged by smart-phone makers and their wireless carriers.

And though many of those companies take a dim view when researchers and hacker groups publicize their vulnerabilities, it's the public that can benefit when those problems are uncovered.

DePetrillo and Bailey were surprised at how easily they could use widely available information and existing techniques to assemble a detailed dossier on a cell-phone user. (They stress that their demonstrations are for educational purposes and that they work better on some cell networks than others.)

Once they have a phone number -- yours, for instance -- they can easily determine your name by taking advantage of a vulnerability in the Caller ID system. Using special software, they can "spoof" a call -- that is, make a call that appears to the phone company as though it's coming from your number. They can then call themselves using your number and watch as their Caller ID device lights up with your name.

Attackers could theoretically do this with thousands of numbers to create

their own personal mobile phone book.

But it doesn't stop there: Once DePetrillo and Bailey have figured out that your name is the one associated with your number, they can query the cellular network to see where your phone is at that moment. After enough time, this bit of digital spycraft will yield a fairly clear picture of where you go and when.

"We can do a lot of cool things that we really shouldn't be able to as civilians," DePetrillo said. "It's like running your own private intelligence company."

Representatives from AT&T and T-Mobile referred questions about the issue to the CTIA, a wireless industry association, which said U.S. wireless carriers are vigilant about protecting subscriber privacy, and questioned whether DePetrillo and Bailey's tracking techniques were legal.

The vulnerabilities in the networks that track phones and connect calls are mirrored by security weaknesses in the phones themselves, one of which is the software they run.

All of the major smart-phone makers have created online markets where users can download any of tens of thousands of small programs -- called apps. On the iPhone, there's the App Store; for Google Android, there's the Android Marketplace; and for BlackBerry, there's the App World.

Those stores have varying levels of policing. Apple certifies the security of every app it approves for its store -- there are now 250,000 of them -- but acknowledges that some malicious apps can occasionally sneak through. RIM and Google largely leave users to protect themselves from the bad guys.

Tyler Shields, a computer security researcher who specializes in mobile phones, likes to show off a nasty little application he wrote called TXSBBSPY.

The "TXS" part is his initials. "BB" is for BlackBerry. And the "SPY" is for the way his program can turn your device into a mobile surveillance station, with you as the target. Once installed on your BlackBerry, Shields' app would let him read your text messages, listen to your voicemails and even turn on your phone's mic while it's in your pocket.

Though Shields' app is intended to be a case study on BlackBerry security, he said an attacker could easily hide similar features in an app masquerading as something else, like a program to do online banking. If a user unwittingly downloaded the phony banking app, his or her device could quickly become compromised.

Because smart phones are only a few years old, Shields said, the art of smart-phone defense is still catching up to where the PC has been for years.

"We're still in the late '90s when it comes to security on mobile devices," Shields said. "It's akin to the older days before people knew to put antivirus software or firewalls on their computers."

For their part, RIM and Google say they have built some precautions into their phones to help users determine whether an app is legitimate. BlackBerry phones offer a set of controls that allow users to prevent apps from accessing some of the device's functions -- such as its messaging and telephony features.

Similarly, before a user loads an app from Google's Android store, the device will display a list of the data to which it has access. If a tic-tac-toe game is asking to access your text messages, that could be a warning

sign.

Google, RIM and Apple all say they remove offending apps from their stores when they become aware of violations. Still, they say, it's up to users to be vigilant when downloading apps -- and to judge whether they're coming from a trusted software maker.

Charles Miller, the principal security analyst at Independent Security Evaluators in Baltimore, stressed that common sense is often the best defense against malicious attacks.

"For 10 years, people have been told all of these things you should do to protect your computer: Don't click on links in e-mails and only go to sites you trust," he said. "People tend to forget those when you're on your phone."