UC SANTA BARBARA

THE Current

July 30, 2014
Sonia Fernandez

Can You Trust That App?

You're on your smartphone, browsing through Facebook. In a fit of productivity, you search for, say, a project management app to help you use your non-Instagram and cat video time more effectively. You download and install the first one you come across … only to find that it doesn't do anything. No reminders, no calendar, no clock, nothing.

Oh, well. You exit the app and go back to Facebook.

Sounds innocuous enough, right? What you might actually have done, however, is give a hacker access to your phone and all the important pieces of information it contains about you, your friends and family. And while the thief's initial take can be relatively small compared to the kind of money he or she can make from hacking into your computer, over time, you could be leaking a lot of money without knowing it.

"The victims of these types of malware and scams could be counted in the hundreds of millions," said Giovanni Vigna, a UC Santa Barbara professor of computer science who specializes in cybersecurity.

Smartphone hacking is one of the fastest-growing issues in terms of cybersecurity, he said, especially with the advent of cloud storage. In Europe, and increasingly in the United States, hackers are able to bypass two-stage identification, whereby a text message is sent to one's smartphone bearing a private code for entry into account websites.

It is a problem that Vigna, computer science professor Christopher Kruegel and researchers from Northwestern University are getting ready to tackle with funding from a $1.4 million grant from the National Science Foundation.

“The thing we’ll be seeing more and more are attempts to violate trust assumptions,” said Vigna, who is a member of UCSB’s Computer Security Group.

And what are these “trust assumptions”?

“Trust is the assurance that a certain application or platform will act as expected,” Vigna said. These are the cues, he said, that prompt the user to drop their guard and volunteer sensitive information. These cues can range from icons on pages that proclaim the authenticity of the site or the security of the download to the very recognizable logos of certain sites and apps.

“People use their phones to click on the Facebook icon, for instance, and the Facebook application starts, and they inherently assume that it’s Facebook running on their phone,” Vigna said. However, he and his team have found that users are also likely to click on a familiar icon that leads to a faux application.

The goal of these stealth attacks is to steal either your money or your information. Money is an obvious motivation, but personal information can be used to steal one’s identity or log in and exploit email or social media. Hackers leverage the trust between accounts in social networks to get the victim’s friends and contacts to click on malicious links.

Among the topics the researchers intend to study is what Vigna calls an “ecosystem of trust” unique to the smartphone world.

“There’s the guy who writes the application, benign or malicious,” said Vigna. “And then he puts it in an app store, so there’s a relationship of trust between those two. And then there’s you, the user, going to the market and downloading one or more apps, and you have some relationship of trust with those. If I’m a benign application developer and I use a certain ad framework to make money from my application, and then that ad framework starts sending malicious advertisements or links to malware, who’s responsible for this? Where’s the trust there? How do you control this trust? How can you be assured that the ad network is going to perform as stated?”

There is some comprehension of the issues, according to Vigna, but there is also a demand for more scientific modeling of these relationships and understanding of what their implications are. That way, flaws can be identified and fixed.

While the issues being studied are applicable to all smartphones, the group will examine trust in the Android world in particular.

“The main point is the tradeoff between openness and security issues. The fact is that Android is a wonderful open platform that allows anybody to do anything — including hacking the cellphones of unsuspecting Android users,” said Vigna. Android’s popular rival Apple iOS, he added, is less penetrable.

The researchers hope to identify not only flaws in the system but also mechanisms to fix or avoid them. Though it’s not guaranteed, they may even develop their own app that can be used to analyze other apps’ behaviors for flaws or potential untrustworthiness.

In the meantime, smartphone users can defend themselves by becoming more mindful of the apps they install, said Vigna. One way to do this is by choosing the better-known app markets and avoiding less reputable third-party sites.

Additionally, the number of downloads can be an indicator of an app’s legitimacy. If something has millions of downloads, it’s likely to be more trustworthy than a similar app with only a few thousand.

Some shady malware developers use intentional typos to entice people into downloading their app, said Vigna. “Angry Birds” becomes “Angry Bords” or some other variation in spelling. It’s clearly not the superpopular smartphone game, but it’s close enough to fool some users into installing it.

And application hygiene is also important, according to Vigna. Often, a user will download an app that promises great things only to be disappointed when it doesn’t work. However, it might be a malicious bit of code that captures user information, so if an app isn’t working as promised, uninstall it.

Of course, to bypass the entire issue of trust altogether, one can simply go low-tech with a cellphone that handles only the basics.

“But then you would be able to do so much less,” said Vigna. Today’s smartphones allow users to do many things they couldn’t before, such as access the world’s

libraries, monitor their fitness and learn a new language.

“Without your smartphone, you wouldn’t have ways to tell your friends where you are all the time and post pictures of embarrassing situations that you would regret later,” he quipped.

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.