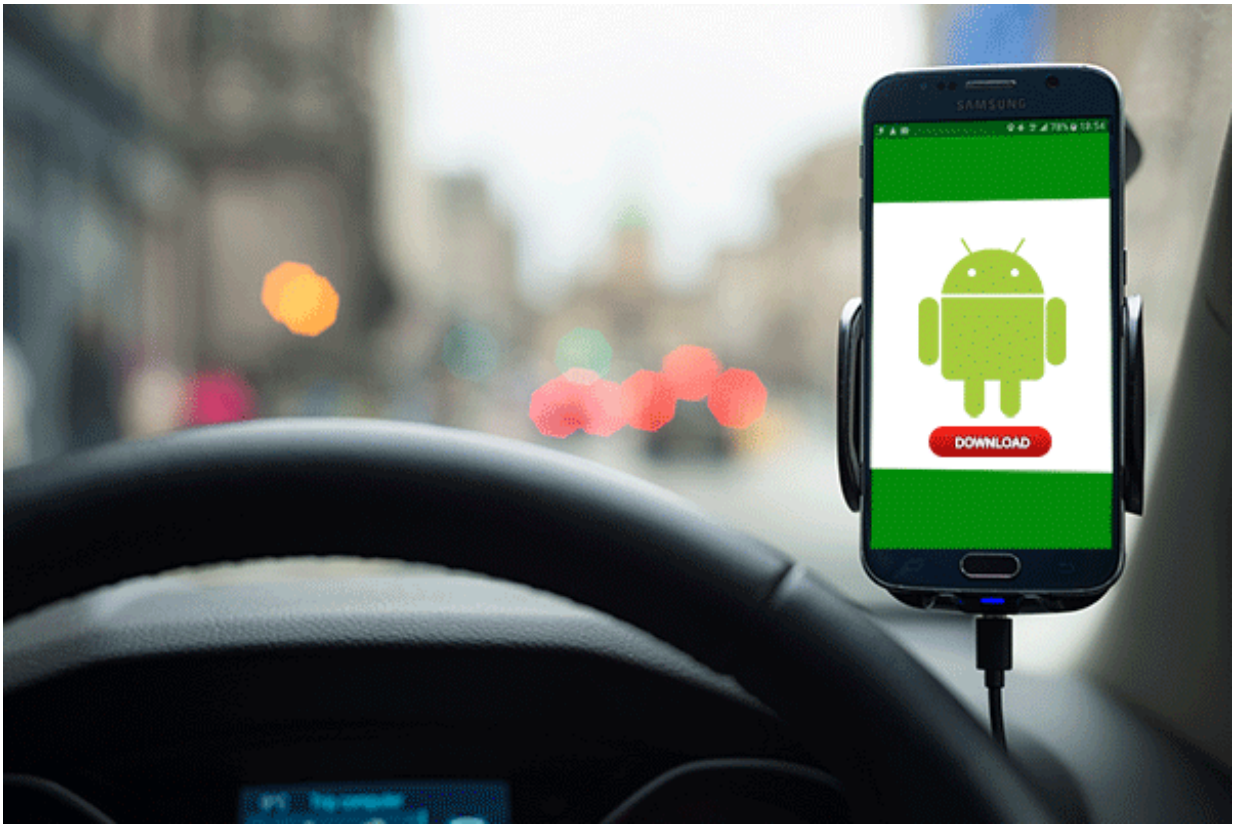
Researchers find that Android apps can secretly track users' whereabouts

August 8 2016



New research led by Northeastern professor Guevara Noubir reveals that some Android apps may automatically transmit sensitive information, such as the routes you travel, through the phone's built-in sensors. A malicious developer, he says, "can infer where you live, where you've been, where you are going." Credit: Younghee Jang/Northeastern University

Three years ago, the Federal Trade Commission dimmed hopes for the Brightest Flashlight app for Android, slapping its developer with charges of consumer deception. Why? The app was transmitting users' locations and device IDs to third parties without telling the users or getting their permission.

Permissions, though, are only a small part of the Android-app privacy story. New research from Northeastern's Guevara Noubir and colleagues shows that Android apps can be manipulated to reach inside your mobile phone to track your whereabouts and traffic patterns, all without your knowledge or consent.

The researchers know this because they built an Android app and tested it.

Their system uses an algorithm that inserts data from the phone's built-in sensors into graphs of the world's roads. The researchers applied the algorithm to various simulated and real roadtrips. For each trip, the system then generated the five most likely paths taken. The most recent results? A 50 percent chance that the actual path traveled was one of the five.

"For $25, anyone can put an app on Google Play, the store for Android apps," says Noubir, professor in the College of Computer and Information Science. "Some of them may be malicious—no one is screening them."

How it works

If an Android app wants to access sensitive user information, such as location, it must let the user know. But often permission for such access is buried in terms-of-use agreements—the small print that many users don't read—or comes up not when the app is downloaded but later,

unbeknownst to the user, when access for that information kicks into gear.

Android apps present further privacy risks because they automatically have access to key sensors inside the phone that detect the device's location, movements, and orientation. Together these sensors can provide clues to everything from the route you take to work to whether you carry your phone in your pocket (the phone is relatively stable) or your purse (it swings).

"In our research we show that an app in fact does not need your GPS or Wi-Fi to track you," says Noubir. "Just using these sensors, which do not require permissions, we can infer where you live, where you have been, where you are going."

The tests

To gauge the effectiveness of the system, the researchers conducted two types of tests.

They simulated drives in 11 cities around the world including Berlin, London, Rome, Boston, and Atlanta. They also got behind the wheel themselves, driving for 1,000 kilometers over more than 70 different routes in Boston and Waltham, Massachusetts. In both tests they collected scores of measurements derived from the phones' changing positions, including the angles of turns and the trajectory of curves.

Their most current results surpassed those initially published in the proceedings of the 2016 IEEE Symposium on Security and Privacy: A 50 percent chance that the actual path traveled was one of 10 generated.

"Inferring a driving pattern from an Android app can lead to much greater invasions of privacy, such as where the user lives and works,"

says Noubir. Additional information, he warns, can then be gleaned by searching town and city public databases for, say, property tax records. "Adversaries can recover lots of details through these side channels."

Protecting yourself

What's an Android user to do short of forgoing apps altogether?

For starters, do your homework, says Noubir. "You should not install apps that are not familiar to you—ones that you have not investigated," he says. "Be sure that your apps are not still running in the background when you're not using them."

He also advises uninstalling apps that you don't use frequently. "Why keep apps that can access your sensors if you don't use those apps seriously?" he asks.

More information: Inferring User Routes and Locations using Zero-Permission Mobile Sensors. DOI: 10.1109/SP.2016.31

Provided by Northeastern University