Researchers develop system to control information leaks from smartphone apps

November 16 2015, by Thea Singer

A research team led by Northeastern's David Choffnes has found "extensive" leakage of users' personal identifying information from apps on mobile devices, including passwords. Their unique ReCon cloud-based system can detect those leaks and give you the tools to stop them. Credit: Matthew Moodono/Northeastern University

If you've used the fitness-tracking app Map MyRun, there's a chance that your password has been leaked.

And the popular fitness app isn't the only one. Other apps may also be putting your information at risk.

A research team led by David Choffnes, an assistant professor in the College of Computer and Information Science, has found 'extensive' leakage of users' information—device and user identifiers, locations, and passwords—into network traffic from apps on mobile devices, including iOS, Android, and Windows phones.

The researchers have also found a way to stop the flow.

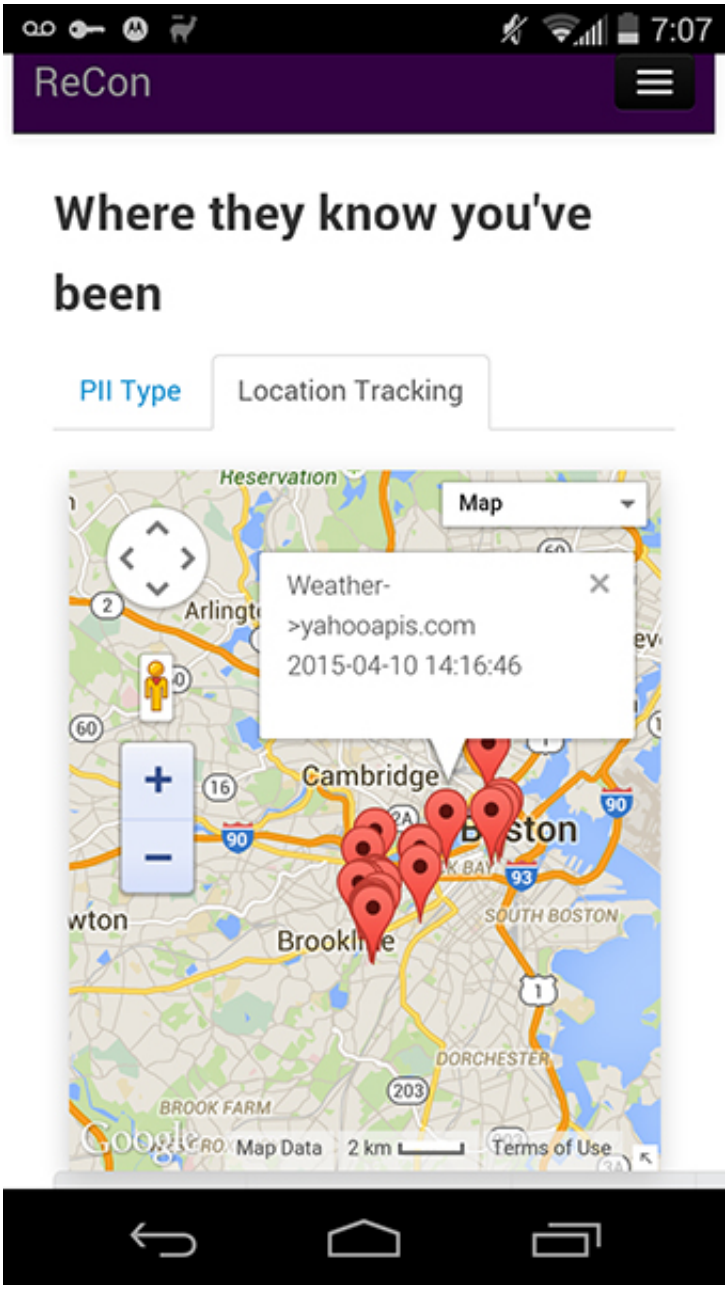
Choffnes will present his findings on Monday at the Data Transparency Lab 2015 Conference, held at the Media Lab at the Massachusetts Instituute of Technology.

In their lab at Northeastern, Choffnes and his colleagues developed a simple, efficient cloud-based system called ReCon with a comprehensive trio of functions: It detects leaks of 'personally identifiable information,' or PII; it alerts users to those breaches; and it enables users to control the leaks by specifying what information they want blocked and from whom.

"Our devices really store everything about us on them: who our contacts are, our locations, and enough information to identify us because each device has a unique identifier number built into it," says Choffnes.

"A lot of network traffic that goes back and forth isn't protected by encryption or other means," he explains. Which may be OK when you submit your email address to an app to, perhaps, subscribe to its newsletter. But not when you type in your password.

"What's really troubling is that we even see significant numbers of apps sending your password, in plaintext readable form, when you log in," says Choffnes. In a public WiFi setting, that means anyone running 'some pretty simple software' could nab it.



ReCon graphically shows users how their locations have been tracked through their apps. Screen shot from recon.meddle.mobi

A June 2015 Forrester Research study reported that smartphone users spend more than 85 percent of their time using apps. But little research has been done on apps' network traffic because mobile devices' operating systems, as opposed to those of laptops and desktops, are so difficult to crack.

Choffnes has changed that. His study followed 31 mobile device users—together they had 24 iOS devices and 13 Android devices—who used ReCon for a period of one week to 101 days and then monitored their personal leakages through a ReCon secure webpage.

The results were alarming. "Depressingly, even in our small user study we found 165 cases of credentials being leaked in plain text," the researchers wrote.

Of the top 100 apps in each operating system's app store that participants were using, more than 50 percent leaked device identifiers, more than 14 percent leaked actual names or other user identifiers, 14-26 percent leaked locations, and three leaked passwords in plain text. In addition to those top apps, the study found similar password leaks from 10 additional apps that participants had installed and used.

In addition to Map MyRun, the password leaking apps included the language app Duolingo and the Indian digital music app Gaana. All three developers have since fixed the leaks. Several other apps continue to send plain text passwords into traffic, including a popular dating app.

Assistant professor David Choffnes has developed a cloud-based system, called ReCon, that gives users control of mobile-app information leaks. Credit: Matthew Moodono/Northeastern University

Using ReCon is easy, Choffnes says. Participants install a virtual private network, or VPN, on their devices—an easy six or seven step process. The VPN then securely transmits users' data to the system's server, which runs the ReCon software identifying when and what information is being leaked.

To learn the status of their information, participants simply log onto the ReCon secure webpage. There they can find things like a Google map pinpointing which of their apps are zapping their location to other destinations and which apps are releasing their passwords into

unencrypted network traffic. They can also tell the system what they want to do about it.

"One of the advantages to our approach is you don't have to tell us your information, for example, your password, email, or gender," says Choffnes. "Our system is designed to use cues in the network traffic to figure out what kind of information is being leaked. The software then automatically extracts what it suspects is your personal information. We show those findings to users, and they tell us if we are right or wrong. That permits us to continually adapt our system, improving its accuracy."

That checks and balances approach works: The team's evaluative study showed that ReCon identifies leaks with 98 percent accuracy.

Apps, like many other digital products, contain software that tracks our comings, goings, and details of who we are. Indeed, if you look in the privacy setting on your iPhone, you'll see this statement: "As applications request access to your data, they will be added in the categories above." Those categories include 'Location Services,' 'Contacts,' 'Calendars,' 'Reminders,' 'Photos,' 'Bluetooth Sharing,' and 'Camera.'

Although many users don't realize it, they have control over that access. "When you install an app on a mobile device, it will ask you for certain permissions that you have to approve or deny before you start using the app," explains Choffnes. "Because I'm a bit of a privacy nut, I'm even selective about which apps I let know my location." For a navigation app, he says, fine. For others, it's not so clear.

One reason that apps track you, of course, so is so developers can recover their costs. Many apps are free, and tracking software, supplied by advertising and analytics networks, generates revenue when users click on the targeted ads that pop up on their phones.

ReCon, alone among app surveillance tools, takes control out of advertisers hands and gives it back to you.

"There are other tools that will show you how you're being tracked but they won't necessarily let you do anything," says Choffnes. "And they are mostly focused on tracking behavior and not the actual personal information that's being sent out. ReCon covers a wide range of information being sent out over the network about you, and automatically detects when your information is leaked without having to know in advance what that information is.

"Finally, which I really haven't seen anywhere else, is this ability to protect your own privacy: You can set policies to change how your information is being released."

More information: Research paper: arxiv.org/abs/1507.00255

Provided by Northeastern University