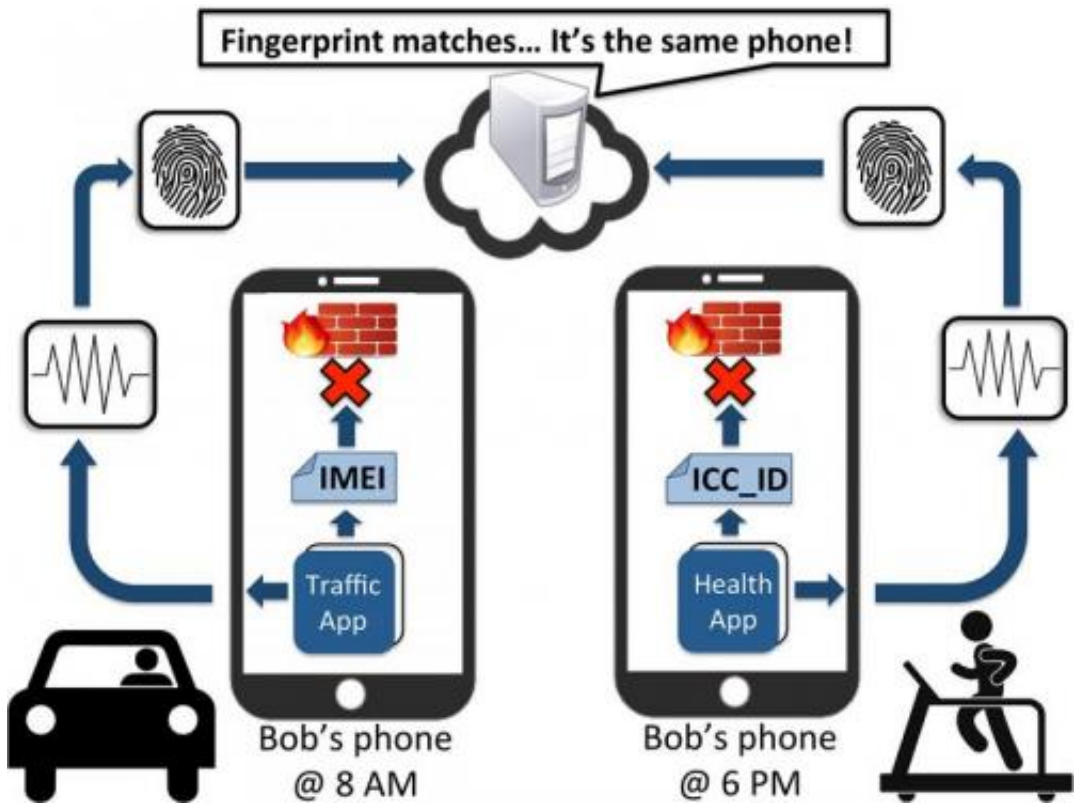
Research shows smartphone sensors leave trackable fingerprints

April 28 2014, by Jonathan Damer



This is an example demonstrating how accelerometer data shared with separate traffic and health applications could indicate Bob's location. Credit: University of Illinois

Fingerprints—those swirling residues left on keyboards and doorknobs—are mostly invisible. They can affirm your onetime presence, but they cannot be used to track your day-to-day activities.

They cannot tell someone in real time that after exercising at the gym, you went to office in a bus and played video games during lunch. But what if our hand-held electronics are leaving real-time fingerprints instead? Fingerprints that are so intrinsic to the device that, like our own, they cannot be removed?

Research by Associate Professor Romit Roy Choudhury and graduate students Sanorita Dey and Nirupam Roy has demonstrated that these fingerprints exist within smartphone sensors, mainly because of imperfections during the hardware manufacturing process.

In some ways, it's like cutting out sugar cookies. Even using the same dinosaur-shaped cutter, each cookie will come out slightly different: a blemish here, a pock there. For smartphone sensors, these imperfections simply occur at the micro- or nanoscale.

Their findings were published at the Network and Distributed System Security Symposium (NDSS). The research also won the best poster award at the HotMobile international workshop in 2013.

The researchers focused specifically on the accelerometer, a sensor that tracks three-dimensional movements of the phone—essential for countless applications, including pedometers, sleep monitoring, mobile gaming—but their findings suggest that other sensors could leave equally unique fingerprints.

"When you manufacture the hardware, the factory cannot produce the identical thing in millions," Roy said. "So these imperfections create fingerprints."

Of course, these fingerprints are only visible when accelerometer data signals are analyzed in detail. Most applications do not require this level of analysis, yet the data shared with all applications—your favorite

game, your pedometer—bear the mark. Should someone want to perform this analysis, they could do so.

The researchers tested more than 100 devices over the course of nine months: 80 standalone accelerometer chips used in popular smartphones, 25 Android phones and two tablets.

The accelerometers in all permutations were selected from different manufacturers, to ensure that the fingerprints weren't simply defects resulting from a particular production line.

With 96-percent accuracy, the researchers could discriminate one sensor from another.

"We do not need to know any other information about the phone—no phone number or SIM card number," Dey said. "Just by looking at the data, we can tell you which device it's coming from. It's almost like another identifier."

Experimental setup showing the external motor used for smartphone rotation. Credit: University of Illinois at Urbana-Champaign

In the real world, this suggests that even when a smartphone application doesn't have access to location information (by asking "this application would like to use your current location"), there are other means of identifying the user's activities. It could be obtained with an innocuous-seeming game or chatting service, simply by recording and sending accelerometer data. There are no regulations mandating consent.

To collect the data, the researchers—as with any would-be attacker—needed to sample the accelerometer data. Each accelerometer was vibrated using a single vibrator motor—like those that buzz when a text message is received—for two-second intervals. During those periods, the accelerometer detected the movement and the readings were

transmitted to a supervised learning tool, which decoded the fingerprint.

"Even if you erase the app in the phone, or even erase and reinstall all software," Roy said, "the fingerprint still stays inherent. That's a serious threat."

At this point, however, there is no absolute solution. Smartphone cases made of rubber or plastic do little to mask the signal. Deliberately injecting white noise in the sensor data can smudge the fingerprint, but such noise can also affect the operation of the application, making your pedometer inaccurate and functionally useless.

The research also suggests that other sensors in the phone—gyroscopes, magnetometers, microphones, cameras, and so forth—could possess the same types of idiosyncratic differences. So even if, at a large scale, the accuracy of accelerometer fingerprints diminishes, when combined with prints from other sensors, an attack could be even more precise.

"Imagine that your right hand fingerprint, by some chance, matches with mine," Roy Choudhury said. "But your left-hand fingerprint also matching with mine is extremely unlikely. So even if accelerometers don't have unique fingerprints across millions of devices, we believe that by combining with other sensors such as the gyroscope, it might still be possible to track a particular device over time and space."

For smartphone users and e-book readers, smartwatch wearers and tablet devotees, perhaps the most critical take-home message, in the short run anyway, is the importance of vigilance.

"Don't share your accelerometer data without thinking about how legitimate or how secure that application is," Dey said. "Even if it's using only the sensor data, still it can attack you in some way. The consumer should be aware."

More information: www.internetsociety.org/events/ndss-symposium-2014

Provided by University of Illinois at Urbana-Champaign