*That Fingerprint Sensor on Your Phone Is Not as Safe as You Think*

The New York Times

Vindu Goel

April 10, 2017

SAN FRANCISCO — Fingerprint sensors have turned modern smartphones into miracles of convenience. A touch of a finger unlocks the phone — no password required. With services like Apple Pay or Android Pay, a fingerprint can buy a bag of groceries, a new laptop or even a [$1 million vintage Aston Martin](http://www.digitaltrends.com/mobile/apple-pay-aston-martin/). And pressing a finger inside a banking app allows a user to pay bills or transfer thousands of dollars.

While such wizardry is convenient, it has also left a gaping security hole.

New findings [published Monday](http://ieeexplore.ieee.org/document/7893784/) by researchers at New York University and Michigan State University suggest that smartphones can easily be fooled by fake fingerprints digitally composed of many common features found in human prints. In computer simulations, the researchers from the universities were able to develop a set of artificial “MasterPrints” that could match real prints similar to those used by phones as much as 65 percent of the time.

The researchers did not test their approach with real phones, and other security experts said the match rate would be significantly lower in real-life conditions. Still, the findings raise troubling questions about the effectiveness of fingerprint security on smartphones.

“It’s almost certainly not as worrisome as presented, but it’s almost certainly pretty darn bad,” said Andy Adler, a professor of systems and computer engineering at Carleton University in Canada, who studies biometric security systems. “If all I want to do is take your phone and use your Apple Pay to buy stuff, if I can get into 1 in 10 phones, that’s not bad odds.”



Full human fingerprints are difficult to falsify, but the finger scanners on phones are so small that they read only partial fingerprints. When a user sets up fingerprint security on an [Apple](http://www.nytimes.com/topic/company/apple-incorporated?inline=nyt-org) [iPhone](http://topics.nytimes.com/top/reference/timestopics/subjects/i/iphone/index.html?inline=nyt-classifier) or a phone that runs Google’s Android software, the phone typically takes eight to 10 images of a finger to make it easier to make a match. And many users record more than one finger — say, the thumb and forefinger of each hand.

Photo

Since a finger swipe has to match only one stored image to unlock the phone, the system is vulnerable to false matches.

“It’s as if you have 30 passwords and the attacker only has to match one,” said Nasir Memon, a professor of computer science and engineering at N.Y.U.’s Tandon School of Engineering, who is one of three authors of the study, which was published in IEEE Transactions on Information Forensics and Security. The other authors are Aditi Roy, a postdoctoral fellow at N.Y.U.’s Tandon School, and Arun Ross, a professor of computer science and engineering at Michigan State.

Dr. Memon said their findings indicated that if you could somehow create a magic glove with a MasterPrint on each finger, you could get into 40 to 50 percent of iPhones within the five tries allowed before the phone demands the numeric password, known as a personal identification number.

Apple said the chance of a false match in the iPhone’s fingerprint system was 1 in 50,000 with one fingerprint enrolled. Ryan James, a company spokesman, said Apple had tested various attacks when developing its Touch ID system, and also incorporated other security features to prevent false matches. Google declined to comment.

The actual risk is difficult to quantify. Apple and Google keep many details of their fingerprint technology secret, and the dozens of companies that make Android phones can adapt Google’s standard design in ways that reduce the level of security.

Stephanie Schuckers, a professor at Clarkson University and director of the Center for Identification Technology Research, was cautious about the implications of the MasterPrint findings. She said the researchers used a midrange, commercially available software program that was designed to match full fingerprints, limiting the broader applicability of their findings.

“To really know what the impact would be on a cellphone, you’d have to try it on the cellphone,” she said. She noted that cellphone makers and others who use fingerprint security systems are studying anti-spoofing techniques to detect the presence of a real finger, such as looking for perspiration or examining patterns in deeper layers of skin. A new fingerprint sensor from Qualcomm, for example, uses ultrasound.

Phone makers have acknowledged that fingerprint sensors are not foolproof, but said that the ease of touching a finger to unlock a phone meant that more users actually turned on security features instead of leaving their phones unlocked — a common habit in the early days of smartphones.

Photo



Aditi Roy, the lead author of a new paper on master fingerprints that could be used to unlock smartphones, examines data on her computer at N.Y.U.’s Tandon School of Engineering.

Credit

Roger Kisby for The New York Times

Dr. Ross acknowledged the limitations of the work. “Most of the current smartphone vendors do not give us access to the fingerprint image,” he said.

For a thief or spy to turn master fingerprints into smartphone keys would require a lot of additional work. “In order to launch this attack, you still have to make fake fingers,” Dr. Ross said.

Still, the team’s fundamental finding that partial fingerprints are vulnerable to spoofing is significant, said Chris Boehnen, the manager of the federal government’s Odin program, which studies how to defeat biometric security attacks as part of the Intelligence Advanced Research Projects Activity.

 “What’s concerning here is that you could find a random phone, and your barrier to attack is pretty low,” Dr. Boehnen said.

Phone makers could easily increase security by making it harder to match the partial fingerprint, he said, “but the average phone company is more worried about you being annoyed that you have to put your finger against the phone two or three times than they are with someone breaking into it.”

Adding a larger fingerprint sensor would also decrease the risk, Dr. Boehnen said. And some newer biometric security options, such as the iris scanner in Samsung’s new Galaxy S8, are harder to trick. (Face recognition, another security option available on some phones, is considered less secure than fingerprints.)

Phone users can also protect themselves by turning off fingerprint authentication for their most sensitive apps, such as mobile payments, Dr. Boehnen said.

Dr. Memon said that despite his research, he was still using fingerprint security on his iPhone.

“I’m not worried,” he said. “I think it’s still a very convenient way of unlocking a phone. But I’d rather see Apple make me enter the PIN if it’s idle for one hour.”

*That Fingerprint Sensor on Your Phone Is Not as Safe as You Think –* Questions

1. How are fingerprints used on smartphones?
2. What is a fake fingerprint?
3. The article states that full fingerprints are difficulty to falsity (or fake), so what is the problem with smartphones?
4. What fingerprint images does a phone take?
5. What is a MasterPrint and what is its potential function?
6. What did Apple and Google say about the chance of a false fingerprint match?
7. Phone makers have acknowledged that the fingerprint sensors are not foolproof, but what do they say are the benefits of the fingerprint system?
8. How could phones increase security?
9. What has Samsung done to raise security?
10. Based on the information in this article, what do you think “biometrics” means?
11. How do you feel about all of this information?