Fingerprint security convenient, but not flawless

February 26 2014, by Anick Jesdanun

The new Samsung Galaxy S5 is examined by a visitor to the Mobile World Congress, the world's largest mobile phone trade show in Barcelona, Spain, Monday, Feb. 24, 2014, after its unveiling. (AP Photo/Manu Fernandez)

(AP)—Samsung's upcoming Galaxy S5 smartphone will be at least the third to have a fingerprint sensor for security but it's alone in letting you use that for general shopping, thanks to a partnership with PayPal.

The sensor brings convenience for entering passcodes and could

encourage more people to lock their phones. But fingerprint security isn't foolproof.

Here's what to know as you consider whether to place your trust in it:

How does it work?

The S5 has a sensor on the home button, just like Apple's iPhone 5s. On the S5, you train the phone to recognize your finger by swiping on it seven times. You also enter a passcode as a backup, so you're not locked out if the device doesn't recognize your print. On the iPhone, that can happen if your hand is greasy or wet, for instance.

The phone then converts the fingerprint information into a mathematical representation, known as a hash, and stores that in a secured location on the device. Samsung says that information stays on the device and is never shared.

When you want to unlock your phone, you simply swipe on the home button. A hash is again created and must match the one the phone already has. Otherwise, the phone stays locked.

You can do this with up to three fingers on the S5, compared with five on the iPhone. On the S5, you must swipe down. On the iPhone, you simply hold your finger on the home button, and you can do that sideways or upside down as well.

The HTC One Max also has a fingerprint sensor, though tests by The Associated Press have shown it to be inconsistent in recognizing prints.

What can you do with the fingerprint?

All three devices let you skip the passcode and unlock the phone.

You can also train the HTC phone to open a particular app automatically depending on the finger used. Apple lets you use the finger to authenticate purchases through its iTunes store, but it's keeping the system off-limits to outside parties. Samsung lets you make PayPal payments.

If you're at a retail store that accepts mobile payments through PayPal's app, for instance, you can use the fingerprint instead of your usual password. That's also the case with online transactions using PayPal on the phone. The hash doesn't get sent to PayPal. Rather, the phone verifies for PayPal that the fingerprint has been verified.

Anuj Nayar, senior director for global initiatives with eBay Inc.'s PayPal business, says there's usually a trade-off between security and convenience. Beef up security, and it's tough to use. Make it convenient, and open up windows for breaches. With fingerprint IDs, he says, you can have both.

Are you really getting security?

That depends.

It's more secure than not locking your phone with a passcode at all. It's also more secure than using a four-digit passcode, as there's a greater chance of guessing that than the particular hash used. But there's never a guarantee.

Shortly after Apple started selling the iPhone 5s, a German hacking group said it managed to bypass the fingerprint system by using a household printer and some wood glue to create an artificial copy of a genuine fingerprint.

The group said the fingerprint ID system was easy to trick, though it's not something easily pulled off in the real world. You need to have that specific phone and the fingerprint, for one thing. And then you compromise only that one phone.

Security experts point out that once a finger's compromised, you can't replace it the way you can a passcode. That doesn't mean someone can use an S5 breach to unlock an iPhone, though, as the hash formulas used are typically proprietary and kept secret.

But it's not a threat to take lightly, either.

"Biometrics work very well for identifying something, but whether you can use it for authentication or not depends on the implementation," says Jeremy Bennett, chief mobile architect for Intel Corp.'s security business, McAfee.

He prefers dual security—using the fingerprint with something else, such as a passcode.

Should you use it?

PayPal officials point out that behind the scenes, it's still performing the usual anti-fraud checks. If the account is used to buy a television in California just five minutes after you buy coffee in New York, it'll suspect something is up.

If the phone is lost or stolen, or your fingerprint is somehow compromised, you can contact PayPal to de-register that device from future use.

Drew Blackard, director of U.S. product planning at Samsung Electronics Co., says other forms of authentication have their flaws, too.

Android phones let you swipe a pattern on the screen in lieu of a passcode, but Blackard points out it's possible to guess the pattern by examining the screen for smudges.

It's not bulletproof security, but it's more secure than existing methods, he says.

Despite the risks, Bennett says he sees potential.

"If it results in more people locking their phone," he says, "it improves security."