iPhone transforms security with fingerprint reader

September 12 2013, by Glenn Chapman

Apple chief executive Tim Cook introduces the new iPhone 5S on September 10, 2013 in Cupertino, California. The 5S is the first phone to feature a fingerprint identification security system, but is likely to be rapidly copied by rivals.

With the swipe of a finger, Apple could jumpstart a new era of smartphone security and strip away fear of tending to banking or other business on mobile devices.

Fingerprint recognition technology built into a sophisticated iPhone 5S set to hit the market on September 20 was hailed by computer security specialists as a welcome move that rivals will likely rally to match.

"It could be amazing," Lookout principal security researcher Marc Rogers told AFP on Wednesday.

"What is going to happen really depends on Apple's implementation," he continued. "We've seen Apple take obscure technologies and make them mainstream overnight."

Apple on Tuesday unveiled two new iPhone models, one of them a top-of-the-line 5S with innovative features including a fingerprint sensor to use as a security measure in place of passcodes.

"You can just press the home button to unlock your phone," Apple vice president Phil Schiller during an event at the company's Silicon Valley headquarters. "You can use it to authenticate iTunes purchases."

Schiller added: "We have so much of our personal data on these devices, and they are with us almost everyplace we go, so we have to protect them."

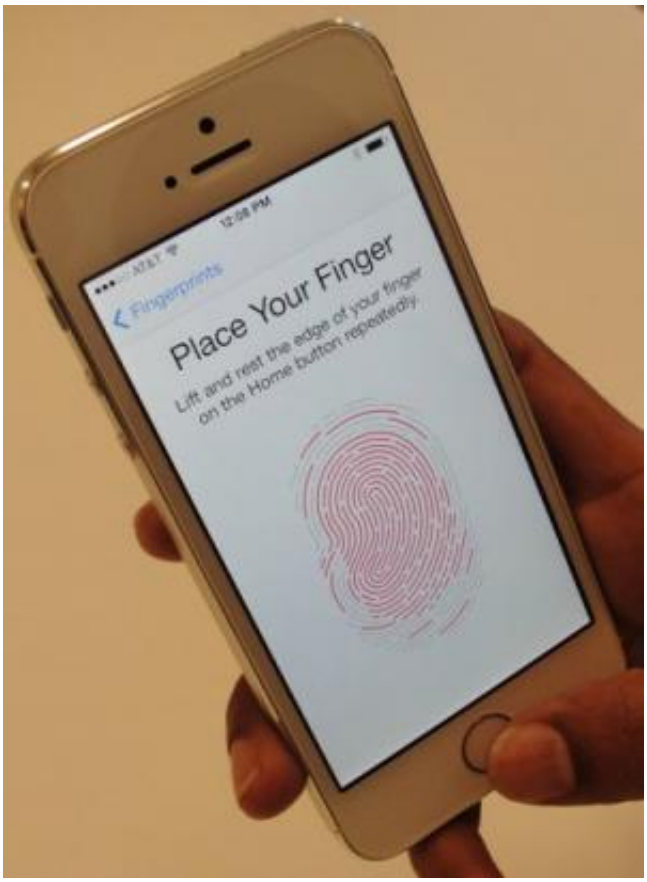
Reticle Research principle analyst Ross Rubin described Touch ID as a "show stealer" that addresses "a necessary annoyance that many consumers have to deal with many times a day."

Studies by Apple and Lookout, which specializes in protecting smartphones and tablets from hackers, show that less than half of smartphone owners protect handsets with access codes

A camera sensor built into the 5S home button at the bottom of the smartphone face peers deep into layers of skin to analyze loops and

swirls of fingerprints.

Data from fingers is stored exclusively inside the sophisticated Apple-made chip that powers the smartphone and is refined every time Touch ID is used, according to Schiller.



A new iPhone 5S handset, which lets the user unlock the phone with a fingerprint, pictured September 10, 2013. Security specialists have hailed the move to incorporate the fingerprint reader, although some fear the technology will be targeted by hackers.

"The company says that fingerprint data is encrypted and not sent to its (or anyone else's - sorry, NSA) servers," security researcher Graham

Cluley said in a blog post, making a reference to reports of US spying on the Internet.

Touch ID lets 5S owners store as many as five fingerprints, meaning people will be able to let spouses, children, or others they trust share access to smartphones.

Combining fingerprint recognition with "second-factor authentication" such as verification codes ramps up smartphone security tremendously, according to Rogers.

"Imagine a banking application that lets you press a fingerprint to gain access, but to transfer money you also enter a four-digit code," Rogers said.

"It could make mobile devices more secure than their desktop counterparts."

Whether Touch ID transforms mobile commerce is likely to depend on how Apple shares the technology with the creators of applications tailored to run on iPhones.

Apple Senior Vice President of Worldwide Marketing Phil Schiller speaks about security features of the new iPhone 5S on September 10, 2013 in Cupertino, California. A camera sensor built into the home button analyses the fingerprint, with each phone capable of storing the prints of five people.

"It is not unreasonable to imagine where Apple might go in the payment space for things outside the Apple ecosystem with a PayPal or Square type function," said Forrester analyst Charles Golvin.

"Some aspect of doing commerce in the real world is on the horizon for Apple."

Computer security specialists note that fingerprint security is not flawless, and resourceful hackers will still craft attacks.

"Your fingerprint isn't a secret, you leave it everywhere you touch," said security researcher Bruce Schneier.

Fooling some of the better fingerprint sensors with rubber fingers is difficult, but possible, according to Schneier, who noted that a researcher in Japan managed the trick more than a decade ago with candy gelatin used to make Gummi bears.

"The best system I've ever seen was at the entry gates of a secure government facility," Schneier said.

"Maybe you could have fooled it with a fake finger, but a Marine guard with a big gun was making sure you didn't get the opportunity to try."

Touch ID also prompted speculation about movie-style scenarios in which someone's digit is lopped off to unlock a stolen smartphone.

Security specialists thought the gruesome tactic unlikely, especially since PIN code access will likely remain in place as a way to get access to a smartphone if something goes wrong with the fingerprint scanner.

"It's inconceivable that malicious hackers and data thieves won't try to subvert Apple's Touch ID fingerprint scanning technology," Cluley said.

"How capable they will be at doing that, remains to be seen."