New iPhone Fingerprint Technology May Be Too Attractive for Fraudsters and Government to Pass Up

September 24, 2013 - In case you hadn't heard, Apple just released the new iPhone 5S for sale. And the company has been touting its ability to use fingerprints instead of passwords for unlocking the phone and for making purchases. At first glance, the technology is pretty cool. But in our opinion it may also prove to be pretty dangerous for users; exposing them to privacy breaches, government snooping and identity theft.

The new iPhone is the first smart phone on the market with a built-in fingerprint scanner. The scanner is supposed to provide a security feature to users with a touch of "cool" associated with it. Instead of using a password to unlock the phone, the owners fingerprint is used.

The owner's fingerprint is encrypted and stored on a chip in the phone. Based on the reading that I've done on this, Apple apparently envisions a world in which fingerprint scans will do a lot more than just unlock the phone. That world will allow iPhone owners to pay for merchandise and access other secure websites by simply touching the phone.

If you think that all sounds great then just consider this. Within days of the launch of the new iPhone, a German hacking group - Chaos Computer Club - announced that it had already cracked the technology. Without going into too much detail, their crack was very simple. They took a picture of the fingerprint they needed, made a negative image of it, printed the negative out on a high resolution printer that used thick ink, and then poured milk latex over it and let it dry. They then used their manufactured fingerprint to unlock the phone and there is no reason to believe that they couldn't have made a purchase with it. Just to make sure that nobody doubted them, they also put two films up on the internet to show the entire procedure (Given the fact that we're against identity theft, we'll refrain from linking to them).

Just to drive their point home, a spokesman for Chaos Computer Club said in a blog post, "It is plain stupid to use something that you can't change and that you leave everywhere every day as a security token." We have to agree but we also have to point out that this particular scenario may not be the largest threat faced by users of the new iPhone.

Any information stored in electronic form can be hacked. Anyone who is walking around with a device that stores their fingerprint data could eventually find that some hacker has figured out how to access their information. And if fingerprints can be used to make purchases, it could be some time before someone who hasn't had their phone stolen actually finds out that someone else has managed to make purchases by gaining access to their fingerprints.

Because the fingerprints are stored on the phone, there is also the question of corporate privacy. Can Apple access that information? If so, what will they do with it? Who will they share it with and why? And what about third party applications that are downloaded to the phone? Will they have access to fingerprint data? These are all questions that need to be addressed.

Fortunately, some lawmakers are already looking at this issue. Sen. Al Franken sent a letter to Apple's CEO Tim Cook asking for some clarification on some of these issues. He also asked a rather frightening question. He wants to know if the stored fingerprint is considered "subscriber information" by the company. If it is, the company can be forced to turn it over to the government with nothing more than a subpoena.

The bottom line here is that using fingerprints in place of passwords would appear to be a risky proposition. In ACCESS opinion, the technology appears to be less secure than passwords and exposes the user to greater risk of privacy invasions, identity theft and government snooping. It is also worth noting that current federal and state laws are not sufficient to protect fingerprint data even under the best of circumstances. So if you are shopping for a new phone, you may want to pick one that secures your data the old fashioned way; with a password.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS