It's Easy to Bypass Smartphone Fingerprint Security

by Sharon D. Nelson, Esq. and John W. Simek

Ever since Apple delivered an iPhone with Touch ID there have been all kinds of ways to defeat the fingerprint sensor. There have been some elaborate (and expensive) methods from using 3-D printing to using Gummi Bears and everything in between. Back in September of 2013, German hacker Starbug successfully proved that bypassing Touch ID was "no challenge at all," according to *Ars Technica*. As Starbug mentioned in the interview, it took him nearly 30 hours from unpacking the iPhone to developing the hack to reliably bypass the fingerprint security.

At the recent 31C3 conference, the folks from Chaos Computer Club demonstrated how easy it was to grab the German Defense Minister's (Ursula von der Leyen) fingerprint through press photos. The photos were taken using only a regular camera. They then used off-the-shelf software (VeriFinger) to take that fingerprint and make an image that ready for printing. It may take some planning to lift someone's fingerprint, but Starbug contends that there are many likely candidates right on the smartphone screen itself and the casing.

An even lower tech attack is to lift the actual finger of the user. Harrison Green, the 7-year-old son of Johns Hopkins University professor Matthew Green did just that. He snuck into his father's room while he was sleeping and pressed his dad's fingerprint on the sensor. No faking or printing required. No software needed, but his attack works one hundred percent of the time. You can't have a better success rate than that. The best part of the story is that professor Green teaches computer security and cryptology.

It's not just Apple. The Samsung Galaxy S5 has a fingerprint sensor too. So does the HTC One Max. As the cost of the sensors keeps coming down, expect to see more and more smartphones equipped with them. Just because your smartphone has a fingerprint sensor doesn't mean that you should use it. Sure it's convenient, but it's not very secure as we've already indicated in the examples.

Since it may take a lot of planning to lift a sample of your fingerprint, most people would think it is a pretty safe way to secure your smartphone. You might agree, but we wouldn't recommend it. In fact, we wouldn't recommend using any biometrics to secure a device. Once your fingerprint, retina, DNA or other biological data is compromised (more correctly the electronic representation of the biometric data) you're toast. In all likelihood, you are not going to replace your fingertips or get an eyeball transplant.

Other than the security issue, there's another reason NOT to use a fingerprint to secure your smartphone. In October, A Virginia Circuit Court Judge has ruled that you can be compelled to give up your fingerprint to unlock your device. Not so with a PIN. A PIN is considered "knowledge" and not something physical. So don't spend that extra money just to get a fingerprint sensor that you probably shouldn't be using in the first place.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com