Consumer Biometrics Month: Why Average Users Shouldn't Worry About Spoofing

Posted on June 23, 2017

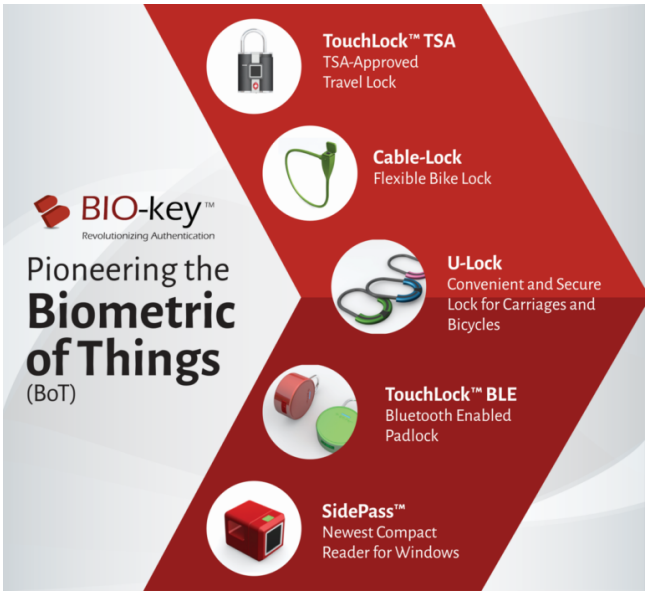
A recent HSBC report cited technophobia as a key obstacle in consumer adoption of new technologies such as biometrics, and while biometry is continuing to proliferate mobile devices to the point of near-ubiquity, there is little wonder why. Successful presentation attacks make major headlines in national and international news outlets every time a hacking group or intrepid journalist successfully spoofs a new device, undercutting trust in the technology most likely to replace passwords. And while breaking through biometric security is newsworthy, illustrating that there really is no perfect security solution as long as there are bad actors aiming to bypass it, the average consumer really has very little to worry about when it comes to becoming the victim of a biometric hacker.

Here's why:

Presentation Attacks On Consumer Devices Are Not Scalable

The most common biometric touchpoint in a consumer's life is her phone. Soon every smartphone available on the market will ship with a fingerprint sensor, and not long after that biometric access will have reached every operational handset, even those without specialized hardware, via software. So, if a consumer is worried about spoofing, the smartphone is the core of that worry. But it really shouldn't be.

The industry standard for consumer mobile biometric access is that biometric template data is stored on a secure element within the



authenticating device. This means no data can be intercepted during the authentication process because it never leaves the phone to begin with. Even if the phone is being particularly unsafe with its data, storing fingerprint images instead of encrypted templates, a remote hack compromising the security on your phone and whatever it protects is nigh impossible. A successful presentation attack on your phone must be done on the device itself.

Herein lies the big drawback of biometrics from a bad actor's perspective: what could possibly be so valuable on an iPhone that one would steal the device, attempt to lift a fingerprint from its surface, and create a workable fake using wood glue or silver ink? The reason passwords are hacked all the time is because it's easy. You can guess them, you can phish them, you can buy them on the dark web. We store passwords in large databases where they can be stolen in bulk. You don't even have to leave the safety of your home office if you want to break into a Gmail account, as was recently explored on a fascinating episode of Gimlet Media's Reply All Podcast, in which the show's producer Phia Bennin successfully phishes both of Gimlet's co-founders who each have SMS-based two factor enabled on their accounts.

In the end, because the ROI of spoofing the average phone is next to worthless, you're much more likely to have a child pick your biometric lock with your own finger while you're sleeping to buy hundreds of dollars worth of Pokemon swag than having your fingerprint spoofed by a hacker who wants to make a quick buck off of your credentials.

You Probably Don't Have an Evil Twin

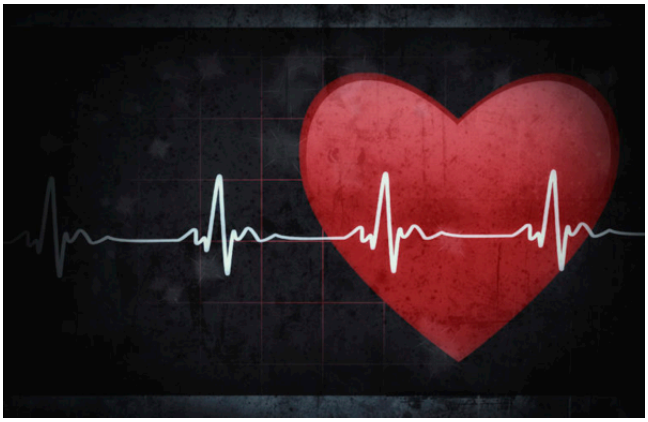
In 2017 the idea of twin-attacks have sprung up in the media more than once. In the world of entertainment, the penultimate episode of HBO's critically acclaimed drama *The Leftovers*, the president of the United States (in an alternate reality) must gain access to a nuclear doomsday bunker using two-biometric factors—facial recognition and something much more private. But an international assassin who also happens to be the president's evil twin brother manages to gain access via false acceptance. His face matches his brother's, as does his more intimate scan, and he gains access.

A more tangible example of a twin attack actually occurred in this reality, when a BBC reporter got his fraternal twin brother to spoof the voiceprint security used by his bank's call center. As our own reporter Alex Perala explained, writing for our sister site Mobile ID World: "While that took several attempts, and most bank customers don't have twin brothers intent on defrauding them, the matter gained some notoriety in the press." HSBC representatives also made the salient point that a twin will likely have little trouble answering traditional security questions based on biographical data, underlining that voiceprint authentication is still the most secure authentication option available over the phone.

It's worth noting that even in the case of identical twins, some popular biometric security offered to consumers, like Windows Hello facial recognition, actually can tell the difference between identical twins. The popular conception that a twin is a living presentation attack waiting to happen oversimplifies the relationship between genetics and physical appearance. It makes for a fun headline and an entertaining hour of prestige television, but doesn't bear too much weight in reality.

Of course, if your identical twin is actively trying to defraud you, you probably have bigger problems to worry about than them trying to use your Samsung Pay account to buy a coffee. But even if that is the case, there are biometrics solutions on the market right now that already have you covered.

Liveness Detection is a Major Priority For the Biometrics Industry



While the vulnerability of the biometrics on your smartphone to presentation attacks should be low on your list of concerns, that doesn't mean it's not a challenge for the industry. As the value of the transaction authenticated by biometrics increases, the greater motivation a bad actor has to spend time stealing your device and making fake body parts in your image. Thankfully, researchers and vendors in the biometrics industry are constantly working to improve liveness-detection—the ability for a given solution to identify a fake biometric, like the wood glue spoof mentioned above, or a video of the user for face recognition.

Notably, Precise Biometrics, one of the leading integrators of biometric matching algorithms for fingerprint scanning smartphones, recently acquired anti-spoofing software specialist NexID. Soon, therefore, we will start to see more robust anti-spoofing capabilities shipping with consumer devices. Furthermore, behavioral biometrics are pulling a lot of weight these days in detecting account intrusions using a variety of minute factors so small they can't be spoofed. Anti-spoofing iris recognition contests are moving eye-based liveness detection forward too.

Very soon, as these advancements come to fruition and proliferate, and

further research and development continues to strengthen biometrics at the consumer level, the already weak arguments against biometric security as a consumer password alternative will cease to hold water. The key will be, as it is now, to help consumers understand biometric security is the safer option.

*

Stay posted to FindBiometrics throughout June as we continue to shine the spotlight on consumer biometrics. Be sure to follow us on Twitter so you don't miss a beat.

> *Consumer Biometrics Month is made possible by BIO-key*

—

June 23, 2017 – by Peter B. Counter

Tags: biometrics, Consumer Biometrics Month, presentation attacks, public perception, spoofing, twins