What is biometric?

Biometric refers to the traits of a human body such as your voice, your face and your fingerprint.

Due to ease of use or user experience point of view, this is incredibly easy to use. However, this is not without its own pros and cons.

Problem with fingerprint

Finger print was commonly used in locking phone devices. Let's first take a look at what a strong password looks like.

"]7g:Yr38b!WX'kV-u&T~B,}!eY68Af&{%!h@#Qt) "
The sample above is a strong password. It's a common knowledge that every human's fingerprint is unique. When we use our fingerprint to lock or unlock phone device. It works by taking our fingerprint then generates strong password. However, you can't replace your fingerprint because your password that was generated by using your own fingerprint can be found or brute force by any malicious attackers.

How can you replace your password that generated through fingerprint? It's only possible if you can replace your fingerprint but in reality.., this is impossible as we know fingerprint can't be changed. Once your fingerprint has been found, there's no way to change it like the good old fashion password.

This is the problem with fingerprint. Ease of use is great and user experience is also great but majority don't understand this critical problem and are fine with fingerprint login or lock/unlock device.

Problem with face and voice

Faces or photos are used to login into to the phone device or lock the phone device. Let's assume this picture below was your face.

Let’s assume that this apple was taken by a cameraman under a hot sun with 100% light and with 10-20% of shadiness. Not to mention that this apple might be 80% ripen and 20% is still not ripe. These factors affect the outcome of the picture photo as each of them contributes to how an apple would like in a picture.

Let’s apply to normal faces as they were used in logging into the phone device? For a moment, let’s say you use a picture of a poker face as a way to logging into the phone device. When you use the picture you may or may not realize the % of the lightness and shadiness and how you pose in the picture.

Regardless if it’s apple photo or the poker face photo, what I am trying to tell you here is that you have to assume that this kind of photo produces a password let’s say “password123456”. Under old school password login mechanism, you have to type exactly “password123456”. However this does not apply here.

What AI or the system will do is to allow some margin of error. If these 2 kinds of photo produce the password of “password123456”, instead of sticking to this approach, what it will do was to allow any password from the range of “password” to “password123456”.

Hence, other apple photo such as 70%-99% light and 30-40% shadiness can be used. The apple may also be ripe at only 60% or 70% and its 30 to 40% may not be ripe yet. The same applies to face photo taken from your face, you may pose similar poses or using lower or higher light concentration instead of the exact photo.

If you reread the password example and the conditions example, you will realize that the criminal or the attacker may not even need to get your face to unlock your device or logging into your account.

The same thing can be applied to your voice as well.

You may start to get the idea that using any forms of biometrics is not really as secure as using a good password or the login mechanism that FIDO uses.

Pros (Advantage)

1. High ease of use and majority will like it
2. Can change any submitted biometrics information if you have bound with your phone number or email address.

Cons (Disadvantage)

1. Social engineering and other applicable attacks will be targeted towards users
2. This poses both security and privacy issues and concerns as it is uncertain how the provider uses these kinds of information or how to properly protect them.