All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The end of biometrics

The main claim about biometrics is basically that they are unalterably unique to the individual. Thus they can, potentially, uniquely and repeatedly identify and authenticate the individual. However, as we look more deeply into this, we find there may be some flaws in this approach.

What biometrics? How unique? How unchangeing? How forgeable? Consent?

Lots of different biometrics of people have been tried. For example,

- **Eye prints, including various ways of seeing patterns of blood vessels, etc.:** Unique so far, not changeable so far, forgeable, no consent
- **Finger prints:** Unique (false +s), intentionally changeable, forgeable, no consent
- **Hand geometry:** Not unique, intentionally changeable, forgeable, no consent
- **EEG and EKG:** Unique so far, always changing, may be forgeable, no consent
- **DNA:** Unique (except twins), not changing, forgeable, no consent
- **Voice print:** Unique (false +s), somewhat changeable, forgeable, no consent

Cutting to the chase, the ones that can change or are not unique make false positives and negatives too common, all are forgeable, and none demonstrate or require consent. Some may debate a few of these results, but together, they form a major problem set for biometrics.

What does the biometric show?

Physical presence of a signal with the identified properties at an interface. Even this is typically either a static signal or a signal that changes in specific known sequences not in response to inputs. A fundamental problem is that once the signal or sequence is known it can be reproduced at the interface. Since there is no muli-party sequence-dependent exchange, biometrics are generally not going to ever be able to address forgery or consent.

Perfection is not the goal

Of course no protective system ever has been, is, or will be perfect. The question at hand is, essentially always, what the tradeoffs are. What is the benefit of the added authentication technology and how effective is it at fending off the threats at hand. The threats at hand are the so-called “design basis threat”, one of the key bases for the design of the protective system. Like the environmental specifications for any engineering design, if we don’t know the nature of the threats we are designing the protective system to operate in, it is similar to designing a bridge without knowing temperature, wind, and earth movement characteristics of the environment it is to operate in.

Since perfection is not the goal, the goal is presumably that we are better and more cost effectively protected with them than without them. The cost is quite low for current fingerprint scanners (inexpensive enough to have them on whole lines of cellular devices as standard features). Facial recognition using built-in cameras is already becoming widespread and is software only on existing devices with video interfaces. The same is true for sound inputs.

So what has changed?

The change in biometrics has come in two ways; (1) biometric devices and their mechanisms have become ubiquitous and (2) other sensors in the world have become far higher resolution and ubiquitous.

- The increasing use of biometrics leads to widespread availability of the technology at low cost and its application for a wide variety of uses. Access to the technology and its detailed implementation is now so widespread that cell phones costing a few hundred dollars include the capability as a matter of course. Like any security technology, its exposure to more circumstances brings out both the benefits and limitations, and it means that attackers have access to the same mechanisms as defenders. Here are some things you may not have been aware of:
    - If I lend you my phone, my finger print interface might just read your fingerprints as you touch the interface to get your biometric information. The same is true for any number of other mechanisms of biometrics. Your exposure to so many of these devices means that any of them might collect the data required to identity, authenticate, and forge your biometric data. Same interface, same data, I just need to use it elsewhere.
    - The mechanisms of biometrics are not limited to what appears at the user interface. Software could intercept or inject false biometrics between the physical interface and its analysis, or from/in storage. Thus software forgery becomes increasingly easy and as Trojan horses are introduced in the ubiquitous environment of biometrics, few if any biometrics may be unavailable to an attacker. Since they are hard to change by the end user (unlike a password) once attained, they can no longer be depended upon for uniqueness. This is the fundamental property we need in order to give them utility.
- The increase of other high quality sensors all over the place leads to the availability of an enormous range of sources of information, including biometric information, that otherwise would not have been available to attackers. Here are some examples you may or may not have been aware of:
    - A recent study identified that a high resolution photograph of a person showing a “peace sign” (2 fingers held up) from about 9 feet away yielded enough information to forge fingerprints. All those cellular pictures taken that include fingers expose the biometric data needed for forgery. Corporate identity badges seen in photographs have been used for many years to create false badges for facility entry as well. Reflected light has also been shown to allow detection of content on screens from around corners and other distant locations. Eye print patterns are likely also detectable from close-up photographs, and with control over a device, even heat signatures of facial components may be readily detectable because of the wide frequency range of many current photographic devices.
    - Recent publications show the detection of sound waves from vibrations in fluids seen in high resolution videos. This allows voice recordings without sound interface and leads to forgery of voice recognition characteristics and even capture of pass phrases as entered via voice.

- Similarly, microphones are now sensitive enough to pick up conversations in other rooms, and people speaking to themselves as they say what they are typing into computers. Historical papers detail how keystrokes can be determined based on the different sounds of different keys and delay between characters with different typing styles and keyboards.

It's far less expensive to make and break biometrics

Crazy as it might seem, the dramatic reduction in cost associated with biometrics has driven them into widespread use at almost no added cost as well as making them easier to defeat. But the question of their effectiveness against a design basis threat remains largely unaddressed. So here is my off-the-cuff assessment of the situation today and as it will progress in the coming years.

- It is reasonably certain that against highly skilled and funded threats, biometrics are not an enormous advantage. They are readily forged or bypassed by highly skilled adversaries. And as time moves forward, the threats will become better at this, and the quality of threat required for exploitation will go down, before long to the level where high school hackers will commonly be able to bypass most commonly used biometrics.
- It is reasonably certain that if someone off the street finds my phone, the fingerprint access control biometric will not be readily bypassed by them. Thus for the average person using a personal device for personal purposes, the simple biometric is reasonably effective and effectively no cost. But so is the password!

I personally like the biometric on my phone. It is faster and more convenient to get access and likely as safe as a password for protecting what's on my phone from the design basis threat I am worried about with respect to my phone. The fact that it occasionally requires a password seems more of an inconvenience than a security benefit. However…

The model may break by being too successful

My cell phone is increasingly being pressed into service as the secondary authentication method for access to other accounts! That's right. The single biometric on my phone now grants access to authenticate my identities on multiple platforms as part of their 2-factor authentication. We keep putting more and more weight on the biometric that was never really designed to take on all that risk. (CAUTION - 4-letter word that ends in "k" just used).

Returning to my conditional: "...for the average person using a personal device for personal purposes...". The problem is that the model will get broken as the devices become ubiquitous and trusted beyond their worthiness. As more and more trust is pushed onto the mobile device authenticated by the same second factor, the consequences of breaking the model increase eventually to the level where it is worth writing and deploying the universal Trojan horse to the mobile device world.

And of course, you can reasonably assume that governments have already figured this out and have placed back doors into these systems for deployment at the hardware and operating system level. So the design basis threat has likely already won.

Conclusion

The end of biometrics is neigh! The King is dead – long live the King! Simply put, you cannot reasonably trust biometrics any more than you can trust passwords, and possible less so.