Zeropasswords

Patented

What's wrong with biometrics?

Nikos Leoutsarakos

Tiny bio

Nikos has a Physics background and a M.Sc. in Computer science from McGill University in Montreal, Canada, where he lives with his wife and two children. He has been publishing and developing systems in the areas of cryptography, wireless/mobility and digital signatures since 1994.

Nikos can be contacted at NIKOS@ZEROPASSWORDS.COM

Prelude

You do not have to be a data scientist to read this paper. If you use a browser to visit your favorite Websites, meet your social media friends online, and check your email daily, this paper is for you.

Let's start by asking: "what happens after you provide a bio-scan to login to a Website?"

Nothing happens. This is a mute question. You cannot login to any Website with biometrics today. Since the early 1970s Websites realized that biometrics requires biometric readers and scanners, which are physical devices that may or may not be connected to browsers everywhere, and they decided to pass and not use this way to login. As it turned out, Websites were correct in refusing to adopt biometrics-based login, but the password-based login systems they chose instead were not much better.

A realization

At closer examination, biometrics-based user identification and authentication systems provide the same protection and suffer from the same vulnerabilities as password-based user identification and authentication systems. The reason being, that both systems are verification systems of shared-secrets. In the case of biometrics, users input something they are and in the case of passwords users input something they know. However, in both cases user input such as PINs, passwords, or retina scans, fingerprints etc. are all converted into bit strings and stored in databases for future verification. Hence, a lot of the vulnerabilities and inherent flaws mentioned in a sister-document titled "What's wrong with passwords?" apply directly to biometrics-based user identification and authentication systems, with 4 additional vulnerabilities outlined below.

1. **Biometrics is not an exact science.** Unlike passwords, biometric readers and scanners generate percentages of resemblance rather than a definite Yes or No. A biometrics-based login system takes a (visual, laser, or capacitive) picture of your finger, retina, palm, ear, face etc. and tries to match it with samples it has previously stored in a database. These samples (originals) in the database were provided by you when you registered the first time. The process begins when the login system converts your bio-sample (e.g. fingerprint) to a set of characteristics (numbers) and then it searches the samples database to find a sample with the same characteristics. Since, it

is virtually impossible to find an exact match of all the characteristics (because you never place your finger on a reader the exact same way twice) it selects the sample from the database with the closest values of characteristics. One can see that this non-deterministic way of comparison and search can produce false positive (or false negative) matches of the input to stored samples. Producing percentages of resemblance is acceptable in some circumstances and totally unacceptable in others. For example, opening doors with your fingerprint and failing occasionally is acceptable, but accessing your money at an ATM machine with your fingerprint and failing occasionally is unacceptable.

2. **You cannot reset your bio.** If, for whatever reason, your password ever gets compromised, it is common practice today to reset it and choose a new one. Unfortunately, you cannot do that with biometrics. You cannot reset your compromised face and choose a new face to use to login. Once hackers have your face pattern, either because they stole the samples database, or because they have a high resolution photo or a 3D rendering of your face, they can impersonate you at will and there is nothing you can do to stop them. Since you cannot change your face, you have no choice but to choose another of your bio-samples to login with. And even then, if for some reason you are the subject of persistent targeted attacks, you will soon run out of fingers, ears, retinas, palms etc. as they, one by one, get compromised! In that respect, biometrics is inferior to passwords because it is finite.
3. **Your bio is public.** As we go about our daily lives we deposit our bio-samples into our environment. We leave our fingerprints on banisters, glasses and coffee mugs; our face and ear patterns are captured by security cameras; hotel bed sheets and pillows are riddled with our dead-skin flakes; our hair falls everywhere; our ECGs are printed on paper or stored in hospital databases, and we are revealing our DNA every time we give blood. Can you imagine doing the same thing with your PIN code or your password, i.e. leaving it all over for hackers to find? Again in that respect, biometrics is inferior to passwords because biometrics is inherently public.
4. **Your bio does not need your consent.** Biometrics-based login systems verify bio-input against stored samples without consideration of the origins of the input. In practice, a hacker can impersonate you using a silicon replica of your fingerprint, or use a high definition photo of your face or ear, use a 3D printout of your palm, or even use

your ECG or your pulse as you lie unconscious or sleeping. Our bio is naturally out of our control. We cannot stop our heart from beating, we cannot hold our breath for ever and we wear our fingerprints and our face on the outside for everyone to see and use. Security-wise, this is a fundamental inherent flaw of our bio because it permits user authentication without user consent.

Conclusion

My objection to biometrics is in the way we use our bio-scans and our bio-behavior to mimic passwords. We store bio-samples and bio-patterns in databases online and then ask users to provide live input every time. We treat biometrics as shared secrets because verification systems function only with shared secrets.

To summarize, there are three problem areas with bio-samples used as shared secrets. First, we expose our online stored bio-samples to the same theft dangers as online stored passwords. Second our bio is not and will never be a secret. And third we have no conscious control over our biology.