CASE STUDY

CYBERSECURITY

4.6.2 - Multifactor Authentication (MFA)

Biometrics

Article:

Can your identity, biometrics, and your privacy get hacked? — Identity Theft Awareness

JUL 30, 2020

Retrieved from: https://medium.com/digital-diplomacy/can-your-identity-biometrics-and-your-privacy-get-hacked-identity-theft-awareness-ee2c6f41b781

Source: Medium
Author: Securelca

We believe in the myth that only traditional password systems can be hacked. But, the fact is, even your face and fingerprints are hackable!

Your identity represents the entire you. It represents your presence in all your activities along. So, if identity is something that only you carry in this world, can it be theft? Can someone take your identity and be you? And if yes, how dangerously can it harm you?

People still have the misconception that biometric authentication such as Touch ID or Face ID can replace traditional passwords and that it could be used to protect valuable information. However, this is far from what the truth is. Biometric is just something we use to convenience the machine about the existence of our identity.

Remember that if your password gets public during any data breaches it could be changed but if the same thing happens with biometric then you can't change your identity, your fingerprint or your face and that's when real trouble begins!!

What is Biometrics?

It is a way to measure a person's physical characteristics to verify their identity. It is a unique way to complete a security-authentication puzzle.

This technology is usually said to be secured when it comes to identification and authentication. And, are used in almost everyday usable devices these days, such as our smartphone, laptops, ATM machine, smart cars, smart homes, and many more.

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Identification answers: “Who are you?”

Authentication answers: “Are you really who you say you are?”

Some examples of Biometrics

Facial Recognition: Technology that measures and matches the unique characteristics of a person’s face for the purposes of identification or authentication.

Iris Recognition: In this type of technology, it measures the unique patterns in the colored circle of your eye to verify and authenticate your identity.

Fingerprint Recognition: This technology allows a person to be verified or identified through the analysis and comparison of his or her finger dermal ridges.

Voice Recognition: This is the ability of technology or program to receive and interpret dictation or to understand and carry out spoken commands.

Can Biometrics be hacked?

When it comes to providing our identity to know who we are it is obvious that we provide some kind of biometrics, but are they truly secured?

Attackers can even duplicate your biometric identification to hack into your devices or accounts.

Any collection of data could easily be hacked and database consisting of a huge amount of biometrics isn’t anything new.

With the advancement of technology and the mind of people, a physical copy of your fingerprint or face could be created from the stored template data.

Stolen data could be reused to gain unauthorized access to a system.

Just like master keys are used to unlock any doors, there is a thing called “master prints” that contain all the standard features found on everyone’s fingers. And attackers can use this to get into devices that use sub-par scanning.

Some Cases Reported

Major breach found in the biometrics system used by banks, UK police, and defense firms. Information such as Fingerprints, facial recognition, and other personal from Biostar 2 discovered on a publicly accessible database. You can read further about the case here[1].

Hackers Make a Fake Hand to Beat Vein Authentication. You can read further about the research here[2].

Researchers at New York creates a tool known as DeepMasterPrints[3], that was used to generate fake fingerprints that can unlock a large number of mobile devices.

Researchers have also proved how deep neural networks could be trained so that the original biometric inputs such as the image of a person's face could be obtained from the stored template data. You can read further about the research here[4].

Through a course of experiments, researchers from Tencent Security's Zuanwu Lab in China came with the conclusion that the ability for facial recognition technology, such as Apple's FaceID, to reliably authenticate that the actual user is not only present but conscious or even alive can be faked. You can find more here[5].

Ways to secure Biometrics

Make biometric authentication as one component of a multi-factor authentication system until sensors and scanners are better able to detect abnormalities.

If you are responsible to store biometric template data, make sure to with secure and encrypted servers and cloud environments.

Know that someone has already discovered the was to assume your facial geometry, fingerprints, and other biometrics and are readily available in the hands of criminals too. You can change your password but not your fingerprints so are aware if you are only using biometric means for security.

Always keep your software up to date if you use biometric verification on one of your devices.

Always be aware of who is collecting your biometric data and for what purpose.

Another way to make biometric systems more secure would be to use blockchain technology.

Conclusion: The technology that is becoming mainstream these days is as equally vulnerable to being theft as it was in the traditional password system. So people must be properly aware and make sure they don't use only biometric authentication as the means to protect their information. This could be used as one of the components in the two-factor authentication.

Summary

Biometrics - the unique physical characteristics of a person - is a tool that can be used for authentication. However, like every other form of authentication, it is not infallible. Some examples include a fake hand to beat vein authentication and software to generate fake fingerprints. To increase security, this article suggests biometrics should be used as part of a multi-factor authentication rather than a standalone method.

Questions

- How should biometric databases be stored; should biometrics also be hashed or should they be stored as they are since they are unique?
- Should a company respond differently to a breach the involved biometrics than just standard hashed passwords? Why or why not?
- In your opinion, should you use biometrics or standard passwords, especially when it comes to breaches that could expose this data?
- Should biometrics be used as an authentication method, or should it only be used as part of multi-factor authentication?
- What are the privacy concerns and issues with biometrics, and should you be concerned?
- Should the government have laws and regulations for how biometrics are stored and/or used?

Further Study

[1] https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms
[2] https://www.eweek.com/security/biometric-security-can-be-hacked-but-it-s-really-hard-to-do
[3] https://www.wired.com/story/deepmasterprints-fake-fingerprints-machine-learning/
[4] https://arxiv.org/abs/1703.00832
[5] https://www.ai-cio.com/news/biometric-hacking-even-face-hackable/