Stuart Hall
ICTN 4040 601
04/10/17

Advantages and Drawbacks to Using Biometric Authentication

As technology advances, so must the means of heightened information security. Corporate businesses, hospitals and your regular everyday people are relying more and more on technology for conducting business, transferring medical records, on-line banking and other everyday activities such as social medial. As the need for stronger information security arises new technology and means of authentication have been created. Multifactor authentication is a means of authenticating an individual using several different forms of authentication. Some use the term three-factor authentication. Three-factor authentication falls into these categories knowledge, possession, and inherence (Haughn, 2014). I consider this as something you know, something you have and something you are.

The category knowledge considers something you know such user-ids, personal identification numbers (PINs) and passwords or passphrases (Haughn, 2014). This is the most basic and most widely used form of authentication. This form of authentication requires that the user “know something” such as a password or PIN. Most everyone who has used a computer, smartphone or computing device is familiar with authenticating by using a password. In most cases the user is required to enter a password in order to gain access or login to a device. In addition to that, most people who use a debit card or credit card have to use a PIN to authenticate to make a purchase or withdraw money from an ATM. PINs and passwords vary in several ways. A password usually requires a combination of letters, numbers and sometimes special characters, whereas a PIN usually only requires numbers. Most PINs are between four to eight digits.

The second category that Haughn (2014) mentions is possession. Possession is "something you have" such as a RSA token or an access badge. RSA tokens usually work together with your password or PIN to become two-factor authentication. For example, when logging into a VPN, you would enter your user-id followed by a PIN plus the token code that the RSA token generated. An example of an access badge would be a physical badge that your employer gives you that grants you access to your building in which you work or even certain rooms/offices within a certain building. When using an access badge you usually have to hold the physical badge up to a scanner and allow it to be scanned. The scanner authenticates you based off of access levels that have been assigned to you and linked to your badge. If you have the correct access levels assigned to your badge, access is granted, if not, you will not be able to enter the building/room as it will not be unlocked.

The last category that Haughn (2014) covers is inherence. Inherence is "something you are". This form of authentication literally uses something you are to confirm your identity. Some examples of this would be a scan of your fingerprint, eye (iris or retina), voice recognition and even your hand-written signature. Requiring a user to enter a password, use a token generated code and a scan of their fingerprint would be an example of three-factor authentication.

Weaver (2006) identifies that there are two subdivisions of biometric authentication: behavioral and physiological. "Behavioral approaches include signature recognition, voice recognition, keystroke dynamics, and gait analysis. Physiological approaches include fingerprints; iris and retina scans; hand, finger, face, and ear geometry; hand vein and nail bed recognition; DNA; and palm prints (Weaver, 2006)".

Biometrics continue to gain support in new technologies and applications across the world. Most smartphones and laptops come equipped with at least a fingerprint scanner for quick authentication and access into said device. Some smartphones even come equipped with eye scanners and facial recognition capabilities.

There are many advantages of using biometric authentication such as, they cannot be lost or forgotten, they cannot be shared with other users, and they are, in most cases difficult to forge. Using biometric authentication could also help reduce operational costs by eliminating the need for users to call into a help desk to have their passwords reset.

If you have ever worked for a help desk then you know that people struggle with remembering their passwords. This is an issue even for people who create simple passwords. Creating simple passwords is not a best practice for any application or technical use. Creating complex passwords is encouraged in most cases but leads to more difficultly remembering and even keying in the correct information. "While forgetting your password is an easy mistake to make, the chances of you forgetting your fingerprints somewhere is, well, nil (PortalGuard, 2015)". This means that you cannot forget your authentication means because it is part of who you are. You cannot forget to take your finger with you to work and the information your fingerprint provides does not change. So there is no need to remember anything. In addition, "fingerprint matching being more advanced and faster than other techniques (Sitalakshmi, 2008).” Operational costs can be reduced somewhat by using biometric authentication. Referring back to the information previously stated that one could not forget their password when using biometrics. This could help reduce call volume into the help desk in which users would need to request that their password be reset and unlocked. That in turn would mean that staffing at your help desk could be adjusted to save on cost.

Another advantage to using biometric authentication is that a user cannot share or transfer that authentication means to another user. One cannot give their finger to someone to authenticate with and they cannot read that information that your fingerprint holds to another user. This information must be scanned and matched to the original scan.

Lastly, biometrics are very difficult, in most cases, to duplicate or replicate. This means that it’s nearly impossible for an attacker to replicate your exact fingerprint into a means that is useable for authentication. “Each fingerprint contains global features, which can be seen with the naked eye, and local features, also called minutia points, the tiny, unique characteristics of fingerprint ridges (Weaver, 2006).” Due to these characteristics and the fact that each finger has around 60 to 70 minutia points, fingerprints become so unique that even identical twins have different minutia points (Weaver, 2006).

Although there are many advantages to using biometrics, there are also a few drawbacks as well. A few of these drawbacks are that if compromised, biometrics cannot be reset, integration and implementation into your business can be very costly, there are sometimes not accurate and can be affected by the environment.

It may be very unlikely, but what if your fingerprint was replicated and someone was able to use it to authenticate as you? At that point, if your only means of authentication was a finger scan, you would never be able to reset it. Therefore, an attacker could continuously use your fingerprint to authenticate as you. The same goes for facial recognition software. In several on-line reviews of Samsung's new Galaxy S8 smartphone, it was proven that you could trick its facial recognition software into authenticating with a photo (Haselton, 2017). In this instance it was very easy to trick the biometric security. Now while other facial recognition software and hardware may be more sophisticated than that found on most common smartphones, it clearly shows that biometrics are not without flaws and can be compromised.

Wang (2009) writes and I quote "simple biometric systems often have many limitations caused by noisy data: susceptibility to spoof attacks, instability of biometric characteristic due to environmental factors or the degrees of freedom offered by feature extraction." This statement confirms that biometrics are sometimes affected by the environment and other factors which could skew readings. For example, in iris scans lighting can affect the accuracy of the scan causing a failure in authentication. "Iris recognition is also very susceptive to many environmental factors especially under noisy conditions (Wang, 2009)."

If you are trying to authenticate using voice recognition, background noise can cause failures in authentication as well. Think about how difficult it is to use voice commands on your smartphone while listening to your radio or while others are around you talking.

Despite the drawbacks of using biometrics, they are gaining more momentum as the advantages seem to out-weigh the disadvantages. Biometrics are continuing to be integrated with more and more technology. They are used in many smartphones, tablets, laptops and desktops and even smart-building at high-tech facilities. Many organizations are starting to use multifactor or three factor authentication and are using biometrics as part of it. If you have the advance software and hardware required to use and secure biometric measurements, your business could benefit greatly from using them. Companies could more securely protect data and information systems as well as reduce operational costs.

References

Haughn, M. (2014, December). What is three-factor authentication (3FA)? - Definition from WhatIs.com. Retrieved April 10, 2017, from http://searchsecurity.techtarget.com/definition/three-factor-authentication-3FA

A. C. Weaver, " Biometric authentication," in Computer, vol. 39, no. 2, pp. 96-97, Feb. 2006., *
from http://doi.ieeecomputersociety.org/10.1109/MC.2006.47
from http://ieeexplore.ieee.org/document/1597098/

PortalGuard, "The Pros and Cons of Biometric Authentication" |. (2016, February 25). Retrieved April 10, 2017, from https://www.portalguard.com/blog/2015/12/22/the-pros-and-cons-of-biometric-authentication/

Sitalakshmi Venkatraman, Indika Delpachitra, (2008) "Biometrics in banking security: a case study", Information Management & Computer Security, Vol. 16 Issue: 4, pp.415-430, *
doi: 10.1108/09685220810908813

Wang, F., & Han, J. (2009). Information fusion in personal biometric authentication based on the iris pattern. Measurement Science and Technology, 20(4), 045501. *
doi:10.1088/0957-0233/20/4/045501

Haselton, T. (2017, March 31). Samsung Galaxy S8's facial recognition can be tricked with a photo. Retrieved April 10, 2017, from http://www.cnbc.com/2017/03/31/galaxy-s8-facial-recognition-can-be-tricked-with-a-photo.html