An Introduction To Biometrics

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

As we are now soon at the start of 2020 Q2, many of the Cybersecurity pundits have already made their predictions as to what the threat landscape will look like. While some have predicted gloom and doom scenarios, others believe that it will be the same as 2019, but only slightly worst.

But there seems to be one common thread with all of these predictions: Despite passwords being the weakest link in the security chain, they will still be the de facto standard that will be used in terms of Identity Management and authenticating end users.

Because of this, the password will still be a highly sought-after item for the Cyberattacker. In a way, this is becoming a cat-and-mouse game. Businesses understand the need to create long and complex passwords, but to employees, they are too difficult to remember. As a result, they resort back to using passwords that can be easily hacked into (such as using "password", or "123456".).

What can be done to alleviate this issue? There some options out there, which include the use of Password Managers. These are software applications that can create and store these long and complex passwords, as well as using Biometric Technology. Also, it is starting to take a precedence in its role as a Multifactor Authentication (MFA) solution, which are the focal points of this whitepaper.

What Biometrics Is All About

Biometrics has actually been around for quite a long time, going all the way back to the 1960s. But it is now until now that it has started to make its splash in the realm of Identity Management. You may be wondering what it is all about? Biometrics is simply another way of confirming the identity of an end user via their unique physiological and behavioral traits. This includes the following:

- Your fingerprint (such as the ridges, whorls, and valleys that are found within it);
- Your hand (this includes the shape of the hand, and the geometric distances between the features of it);
- Your eye (this encompasses both the iris and the retina–the former is the colored region between the pupil and the sclera, and the former refers to groups of blood vessels in the back);
- Your face (this includes the examination of your lips, nose, chin, eyebrows, etc., and the corresponding distances between them);
- Your voice (this is the differing voice inflections in our everyday speech);
- Your signature (note that this is not the signature itself, but in the mannerisms in which we sign our name);
- Your keystroke (these are the mannerisms in which we type on our computer or wireless device keyboard).

The first five are known as "Physical Biometrics", and the last two are known as "Behavioral Biometrics".

How Biometrics Can Confirm Your Identity

Biometrics can be installed in many types of configurations, from being very complex to very simple. Probably the best example of this is the TouchID and FaceID that are used in the latest versions of the iPhone. But no matter what the configuration is, there is a methodology that is used across all the Biometric Modalities in order to confirm the identity of an individual which is as follows:

- Raw pictures and/or samples are collected and converted into various images;
- These images are then combined into one master image;
- From the master image, the unique images are then extracted and evaluated by the Biometric system;
- Once the unique features have been extracted, they are then converted over into a unique mathematical file; this becomes known as the "Enrollment Template" and is permanently stored into the database of the Biometric system;
- If an end user wishes to gain either physical or logical access entry, he or she must go through the first three steps again. The end result is that the "Verification Template" is thus created;
- The Enrollment and Verification Templates are then compared against one another to determine the statistical closeness between the two. If there is a close enough match between the two, the end user is then granted access to the resource that he or she is seeking. If there is not enough closeness, then the individual must start this entire process all over again, from the very beginning.

It is important to note that the first three steps are known as the "Enrollment Phase", and the last two are known as the "Verification Phase".

Biometrics As A Replacement To The Password

As previously mentioned, using a Password Manager is a good option to have in order to enforce your Identity Management Policies. But what about something even better? Well, there is Biometrics. This technology is fast becoming seen as the ultimate replacement to the password.

When Biometrics are used in this regard, is known as a "Single Sign Solution", or an "SSO" for short. The reason why it is called this is because in literally one scan of your fingerprint or iris, you can be logged into a computer or wireless device in just a matter of a few seconds.

Although in theory any Biometric modality can be used as an SSO, it is primarily that of Fingerprint Recognition and Iris Recognition that are being used across Corporate America, whether it is an SMB or even a Fortune 100 company. Facial Recognition is starting to be used, but there are still issues, especially with those related to privacy rights.

An example of a Fingerprint Recognition based SSO is can be seen in the illustration below:

This Fingerprint Recognition device can be installed directly onto your workstation with a USB cable. The red portion on top is the optical sensor from which an end user places their fingerprint on, and where both the Enrollment and Verification processes take place. All that is needed is the appropriate driver which can be downloaded in just a matter of a few minutes. In this regard, Fingerprint Recognition is deemed to be a "full contact" type of technology, in that the end user has to have physical contact with the device.

An example of an Iris Recognition based SSO is also illustrated below:


Iritech, Inc.

This kind of device works exactly in the same manner as the Fingerprint Recognition device as seen previously. But the only difference is that this is a "non-contactless" kind of technology, in that all the end user has to do is merely point the camera (which is the large circle at the top of the device) in front of their eye at a reasonably close proximity so that a good quality image of the iris can be captured.

It is important to note that both of these devices illustrated are external devices, in many computers and wireless devices today, these kinds of cameras and sensors are actually embedded into the hardware themselves.

There are a number of key advantages as to why organizations should seriously consider adopting Biometric based SSOs versus using the traditional password as the primary means of confirming the identity of an individual:

- Unlike passwords, your fingerprint or iris cannot be stolen, they are a permanent part of you;
- Just about every human being on the planet as their own unique set of fingerprints or irises– therefore they cannot be replicated, unlike a password;
- Because the Enrollment and Verification Templates are actual mathematical files, there is nothing that a Cyberattacker can do with them in the case that they are hijacked, unlike with stolen passwords or credit card numbers;
- It is quite difficult to reverse engineer these mathematical files in order to construct the original composite images of either the fingerprint or the iris;
- An end user can literally be logged into their workstation or wireless device in just a matter of a few seconds, versus the minutes it can take to use a password. Although this time gap may not appear to be too significant, the time savings can add up in the long term, and thus result in greater employee productivity;
- In most businesses, the typical administrative cost to reset a password is about $400 per year per employee. A Biometrics based SSO totally eradicates this cost;
- Because employees will no longer have to remember long and complex passwords, the so called "Post It Syndrome" is also totally eliminated. This is the situation where the employee writes down their password, and sticks it their workstation monitor so that they can remember it more easily;
- As mentioned, since everybody has a unique fingerprint and iris structure, by using them as an SSO, the overall security posture of a business is further enhanced because passwords are no longer needed and thus not being used;
- Fraud is also becoming a huge and escalating reality, but by using Biometrics based SSOs, this should help to bring these levels down drastically, because after all, nobody can replicate your fingerprint or iris.

What is Multifactor Authentication?

Multifactor Authentication can be specifically defined as follows: "[It is] a security system that verifies a user's identity by requiring multiple credentials. Rather than just asking for a username and password, MFA requires other—additional—credentials, such as a code from the user's smartphone, the answer to a security question, a fingerprint, or facial recognition."

(SOURCE: 1).

As can be discerned from the above definition, the basic premise is that deploying at least three or more layers of defense has a much higher statistical probability of thwarting off a Cyberattacker than just having one or two layers of it. In other words, the likelihood that a Cyberattacker will reach their ultimate target will diminish each and every time that they break through a line of defense. Thus, in the end, having as many layers of security as possible is the best scenario for any business or corporation when it comes to protecting their IT assets, primarily that of the Personal Identifiable Information (PII) of their customer base, as described earlier.

It is important to note that the Layered Security approach can be used in both Physical Access and Logical Entry applications, but it is typically much more deployed for the latter scenario, especially when it comes to Network Security.

The Functionalities of Multifactor Authentication

Now that we have laid down the groundwork for what an MFA Solution is supposed to do, there are three specific functionalities to it, or in other words, how it should operate in a real-world environment. They are as follows:

1) What you know:

   This can be deemed as a "Knowledge Based" form of Authentication. In this type of scenario, the individual has some intimate insight into themselves that can be used as a form of identification. The most typical example of this is the traditional password. This has been used as probably the most widely used form of authentication for decades. Because of this, it has been a long, sought after item for the Cyberattacker, because once this is hijacked, he or she can then gain access to all kinds of private information and data, especially those that are financially related, such as credit card numbers and other kinds of banking/investment details. A step up from the password is the Challenge/Answer question response, in which the end user can choose from a series of preestablished questions and create their own answer for that. A common example of this are questions like "What is your mother's maiden name?", or "Which was your high school mascot?"

2) What you have, or own:

   This is very often viewed as a "Possession Based" form of Authentication. With this, the end user actually owns a specific item, or at the very least, is in possession of it which can be used to confirm their identification. Typical examples of this include those of physical kinds of tokens, such as Smart Cards, electronic based FOBs, and even the popularly used RSA Token. The main disadvantage with this kind of approach is that these devices are typically very small in nature, and thus, they can be lost or stolen quite easily.

3) What you are:

   This is a feature that you physically own, on your own body or behavior. Examples of this include your fingerprint, face, eyes, voice, hands, and even blood vessel patterns. These are physiological traits. In terms of behavioral aspects, this can include the way you sign your signature, and even the way you type on a keyboard. In fact, these are all probably the best form of authentication is only unique to you, and they cannot be stolen or even replicated. The

technology that encompasses this specific realm of Multifactor Authentication is known as "Biometrics" and will be examined in more detail in the next section of this whitepaper.

Despite the limitations of these individual forms of authentication, if they all three were to be used together as a Multifactor Authentication solution, then the Cyberattacker would obviously have a much harder time in trying to break through the lines of defenses. In fact, a newer form of Multifactor Authentication that has just started being used is known as "Adaptive MFA".

In this configuration, the IT Security Team of a business or a corporation can decide when an MFA approach is needed, who needs to present this level of identification, and the types of authentication functionalities should be used (as just described). In other words, this is more of a dynamic approach to confirming the identity of an individual, depending upon the circumstances that are present at that moment in time, rather than taking a static, or "one size fits all" approach.

By incorporating the principles and concepts of Artificial Intelligence (AI), this newer form of Multifactor Authentication even considers the following variables:

- Where you are trying to access to;
- When you are trying to gain access;
- The kind or type of authentication mechanism that are using (based from the three categories reviewed);
- The kind of network that is being accessed, for example, whether it is a public or private network.

It is important to note that many businesses and corporations still have not embraced yet this MFA approach. Rather, these entities rely solely upon a subset of it, which is known as "Two Factor Authentication", or "2FA" for short. Although this provides a stronger means of authentication as opposed to just using one, this kind of set up is starting to erode quickly, as Cyberattackers are becoming much more sophisticated in nature.

Thus, what is needed is a robust layer of authentication – something that cannot be stolen or replicated. This is where Biometrics comes into play and is reviewed in the next section.

Biometrics In Multifactor Authentication

When it comes to using Biometrics as a layer in a Multifactor or even a Two Authentication approach, the two applications in which it is widely used the most are in Physical Access and Logical Access entry scenarios. With the former, the end user (or the employee) can use their ID Badge (which is most likely a Smart Card) in order to gain a first level of access into the business or corporation. From there, then he or she can then gain further access into other, more secure parts of the organization via a Biometric modality.

With the latter, the password or some kind of established PIN Number is used in order for the employee to first login into their workstation or wireless device, then a Biometric modality can be used to gain access into the more sensitive parts of the IT and Network Infrastructure, such as gaining access to shared resources and other more sensitive applications and documents on the network drives. In these instances, typically Fingerprint Recognition and Iris Recognition are used the most and are further described in the next two subsections.

Fingerprint Recognition

This kind of Biometric modality has been around for a very long time, in fact even going back as far as the 1960s. In fact, it has become the de facto standard when it comes to confirming the identity of a particular individual. It is still a full contact kind of technology, in that the end user must place their fingertip directly onto an optical sensor. But the technology is advancing to the point now that even non contactless forms are starting to come out into the marketplace, in which the individual now only has to present their fingertip at a very short distance in front of a camera.

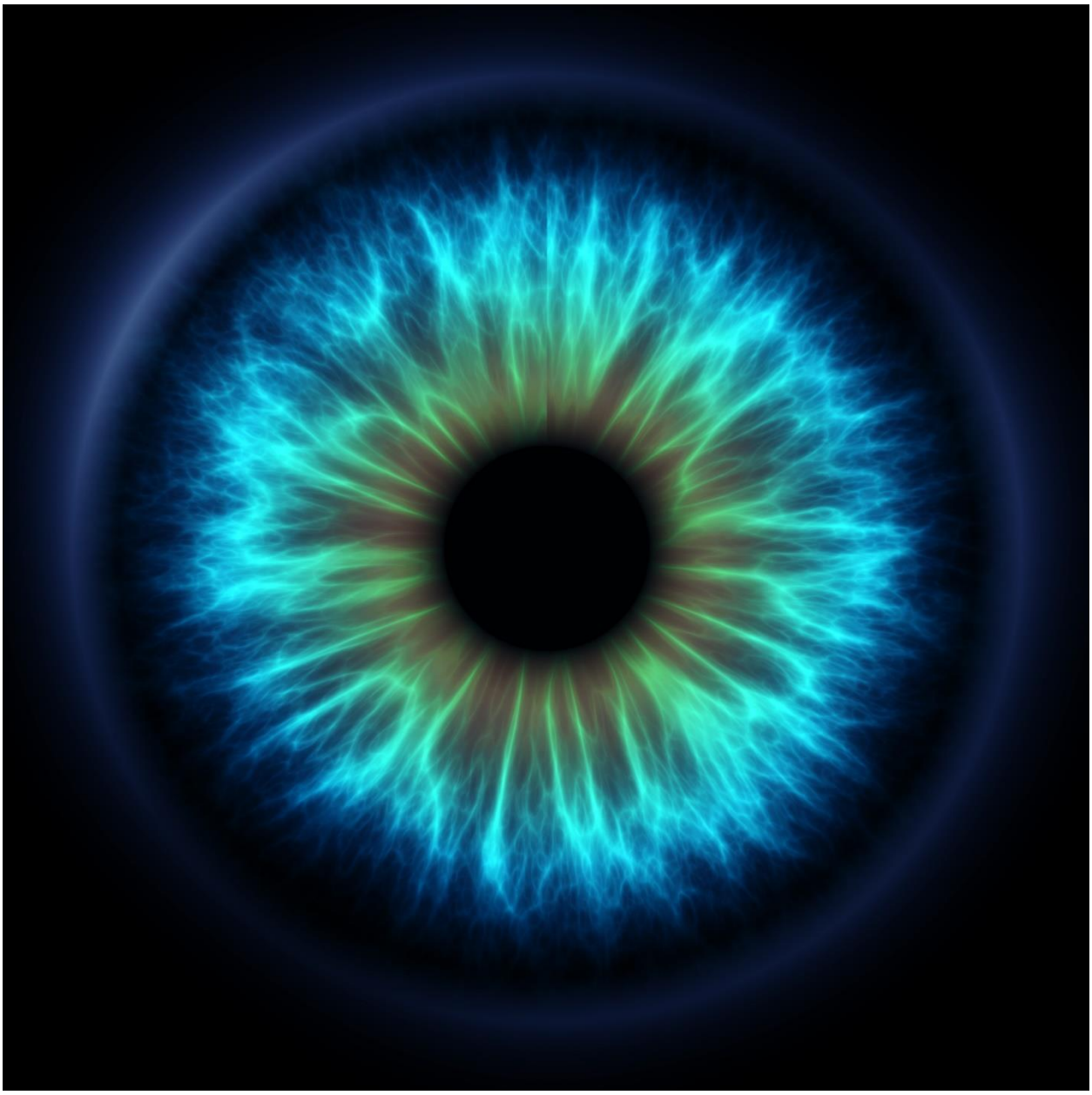
When an image of the fingertip is first taken, it gets converted into a binary mathematical file, which is nothing really but a series of zeros and ones. For example, it will look like this: 00001010101111100001. This becomes known specifically as the "Enrollment Template" and is stored permanently into the database of the Biometric device.

When the end user wishes to gain access to something that requires a further, or secondary layer of authentication (exclusive of a password or PIN Number), the end user must present their fingertip again. During this process, a second image of the fingertip is taken again, and it too gets converted over into a binary mathematical file. This becomes known as the "Verification Template".

But in order to be fully authenticated by the Fingerprint reader, the Enrollment Template is compared against the Verification Template. If there is enough of a statistical closeness between the two of them, the end user is then granted access to the resources that they are seeking to use. It is very important to keep in mind that there is never such a thing as a 100%, identical match between the Enrollment and the Verification Templates; that is why only the correlation, or closeness between them is examined.

Also, the binary mathematical file is a derivation of the unique features that are extracted from the fingertip. These include the whorls, ridges, and valleys that can be seen on the tip of the fingertip. But there are also other forms of unique features, and these are referred to as the "minutiae". These are the simply the breaks, and discontinuities that exist, but cannot be seen by the naked eye.

With this type of Biometric modality, the iris of the eye is used as a means to confirm the identity of the individual. This is the colored region that lies in between the pupil and sclera of the eye, which is also known as the "white of the eye". An image of the iris is illustrated below:



Iris Recognition also follows the same processes of Enrollment and Verification Template as well as examining the statistical correlation between the two as in Fingerprint Recognition. But there are two primary differences in this regard, and they are as follows:

- The unique features are different. For example, there are quite a number of them which are known as the furrows and freckles. Through the Iris scanner, these appear as dots and other irregular, shaped forms. But these are not extracted, rather it is their mathematical vector orientation with respect to the iris that is extracted.
- The mathematical files that are used to create both the Enrollment and Verification templates for the Iris are much more complex. For instance, they rely upon a branch of mathematics known as “Gabor Wavelet Theory”. From there, the respective templates then become a hexadecimal file format, which is illustrated below:

```
:100000000C942A000C9434000C9434000C943400AA
:100010000C9434000C9434000C9434000C94340090
:100020000C9434000C9434000C9434000C94340080
:100030000C9434000C9434000C9434000C94340070
:100040000C9434000C9434000C9434000C94340060
:100050000C94340011241FBECFE5D8E0DEBFCDBF25
:100060000E9436000C9445000C9400008FEF87BB73
:100070002CE231E088B3809588BB80E197E2F901FA
:0E0080003197F1F70197D9F7F5CFF894FFCF3C
:00000001FF
```

(SOURCE: 2).

When compared to Fingerprint Recognition, Iris Recognition has now evolved completely into a non-contactless form of technology. This simply means that there is no direct contact required by the Iris scanner, all the end user has to do is just stand a mere few inches away from it in order to capture an image of their iris. But the technology has evolved to the point now where an Iris Scanner can even capture the iris image of an individual from a very far distance, thus it is now being deployed in large scale settings, such as those of international airports.

Conclusions

Overall, this whitepaper has examined what Biometrics is, and how they can be used as an Identity Management platform, especially when it comes to replacing the password, as well as solution for Multifactor Authentication (MFA). The two most dominant modalities that will be used for both of these types of applications will be that of Fingerprint Recognition and Iris Recognition, primarily because of the following:

- Ease of use;
- Ease of deployment;
- Short amounts of training required for the end user (the employees);
- Affordable costs.

Other modalities will eventually be used, such as Facial Recognition. But it still has some barriers to cross, especially when it comes to the social issues of Civil Liberties and Privacy Rights violations.

Sources

1) https://www.onelogin.com/learn/what-is-mfa
2) https://ucgeeks.wordpress.com/2015/04/19/understand-hex-file-formate/