ROOTSTRAP

Biometrics & The Zero Trust Framework

Authors

Anthony Figueroa is the CTO & Co-Founder of Rootstrap that has built innovative solutions for MasterClass, Google, and Salesforce that help solve their most pressing business challenges. He loves world-changing technologies, building relationships, and solving complex problems. He's passionate about bridging the gap between business and technical strategy. His mission is to help companies create impactful digital products that delight users.

Patrick Ward is the VP of Marketing for Rootstrap, a custom software development consultancy that digitally transforms companies like MasterClass & Google, along with A-List Celebrities like Tony Robbins & Snoop Dogg, and the Founder of NanoGlobals, an expert-led platform that helps mid-size tech companies tap into global markets through remote hiring, offshoring, and international market expansion.

A writer by trade, Patrick's international brand & B2B marketing expertise has been featured in The New York Times, Ad Age, Fast Company, Morning Brew, Hacker Noon, HuffPost & Business Insider.

Ravi Das is a Cybersecurity Consultant and Business Development Specialist. He also does Cybersecurity Consulting through his private practice, RaviDas.Tech, Inc. He is also studying for his CompTIA Security+ Certification.

Table of contents

Introduction: Our Nemesis - The Password

Since the advent of technology, there has been one common denominator that has been a great impediment to further growth: The Password. Whether we love it or hate it, the Password has been the de facto standard for both authentication and authorization purposes. There was a time when cybersecurity as a concept and digital security breaches were inconceivable. Due to this phenomenon, society as a whole had complete faith that the Password would be the ultimate key to securing just about anything.

Fast forward many years later, the opposite is now becoming true: the Password has become the nemesis of the modern digital world. Not only is it the highly coveted piece of information on a potential victim for the would-be cybercriminal, but the general population is now fighting against all of the security policies that were initially put in place to protect them.

For example, corporate employees are often prone to reusing the same passwords over and over again, going so far as to share them with others or even attach a post-it note containing them to their screen monitors which has become affectionately known as the “Post-it Syndrome”. Human beings are merely creatures of habit. We simply do not wish to change unless we are compelled, and even then, we will do so begrudgingly, cherishing the days of comfort when we had something we knew, and more or less trusted.

We will change with a huge and heavy heart, even despite being shown the advantages of a new solution. Probably the best example of this is the Password Manager. Even despite the ability of this software package to create long and complex passwords, and even remember them, and reset them on a pre-established schedule, companies still struggle to gain widespread adoption of this software solution by their employees. Compelling employees to use Password Managers can work in the short term, but longer term, even this strategy is likely to backfire.

Due to the ever present threat of cyber attacks in conjunction with this employee reticence, many companies have been scrambling to find new alternatives to replace passwords. While there are some solutions in place, the truth of the matter is that they likely will never be adopted as a replacement standalone solution.

Rather, these solutions will be used in conjunction with passwords, as a means to provide what is known as Two Factor Authentication (2FA) or Multi Factor Authentication (MFA). One such architecture that is now evolving to varying degrees (and actually proving to be successful) is that of the Zero Trust Framework (ZTF).

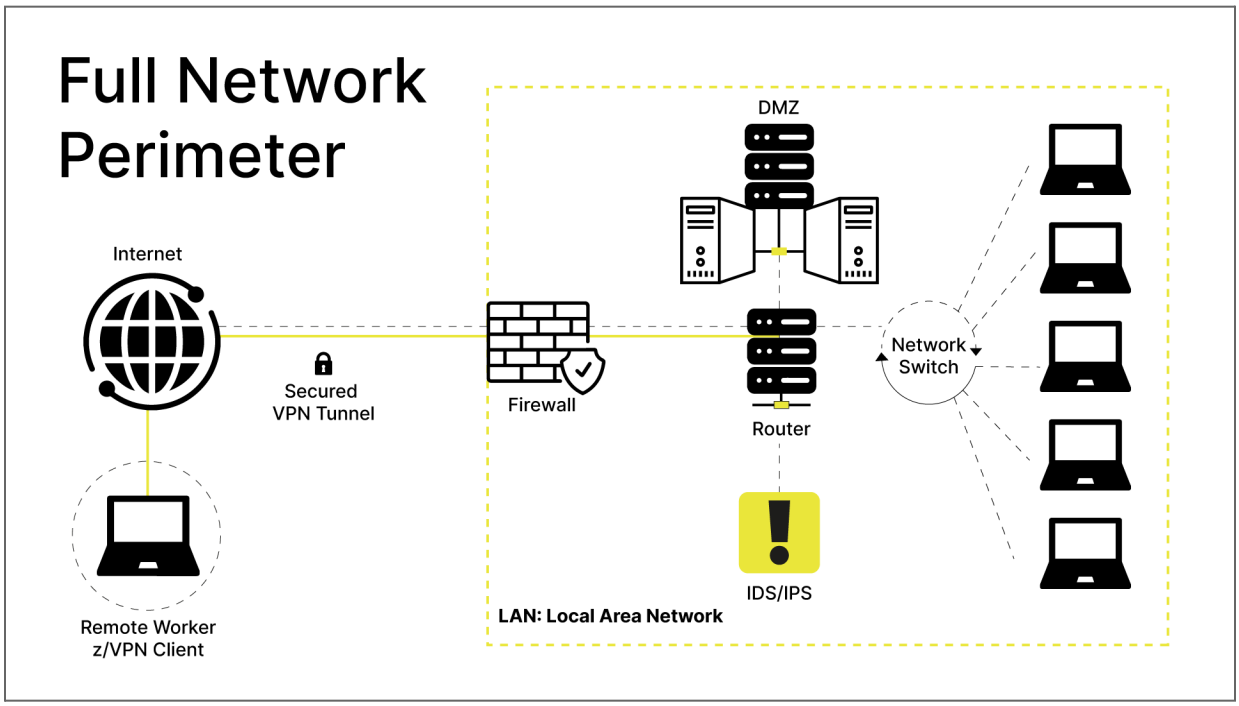
Apple, a perennial pioneer in the security space, has started its own endeavor to get rid of The Password. At WWDC 2022, they presented Passkeys using Touch ID and Face ID. Passkeys is being introduced in MacOS Ventura and iOS16, with technology developed in conjunction with Google and Microsoft through the FIDO Alliance. The technology underpinnings are unique codes generated for apps and websites. Users log on by selecting a passkey, instead of using a password. Since the passkeys aren’t stored on servers, they can’t be hacked. According to Apple, this makes them safer than 2FA. Passkeys can be securely synced across devices (Mac, iPhone, Apple TV) with e2e encryption. Google is using the same approach, as demonstrated at Google I/O in May 2022.

The Premise Of The Zero Trust Framework

The Perimeter Security Approach

As its name implies, the ZTF is one in which nobody is trusted, in both the internal and the external environments. There is absolutely no level of implicit trust here, and when it comes to the corporate environment, employees can not be trusted, regardless of tenure. If the approach sounds extreme, that’s because it is. This approach has been designed for the modern world’s ever-changing dynamics of the cybersecurity threat landscape, and at this point, our hands are tied.

Previously, many businesses have relied upon



[FIGURE A] (Source: https://digital.com/best-vpn-services/what-is-perimeter-security-architecture/)

what is known as "Perimeter Security" (see Figure A). This is essentially one circle of defense completely surrounding the organization, and literally, all manners of security technology is incorporated to defend the corporate entity (think firewalls, network intrusion devices, routers, and any other security device imaginable). The logical fallacy is that since the organization is extremely well fortified, the company assumes that it is totally protected. A hypothetical: what if the cybercriminal actually breaks through this unilateral line of defense? Gaps and weaknesses always persist, even in the most advanced of security tools. Once a breach has occurred, the cybercriminal has free rein to all of a company's digital assets. In other words, there is no multi-layer of security here, which lessens the likelihood of the cybercriminal from accessing a company's most sensitive information at each point of entry. A company may have installed 2FA or MFA, but that won't be sufficient if there is just one layer of defense.

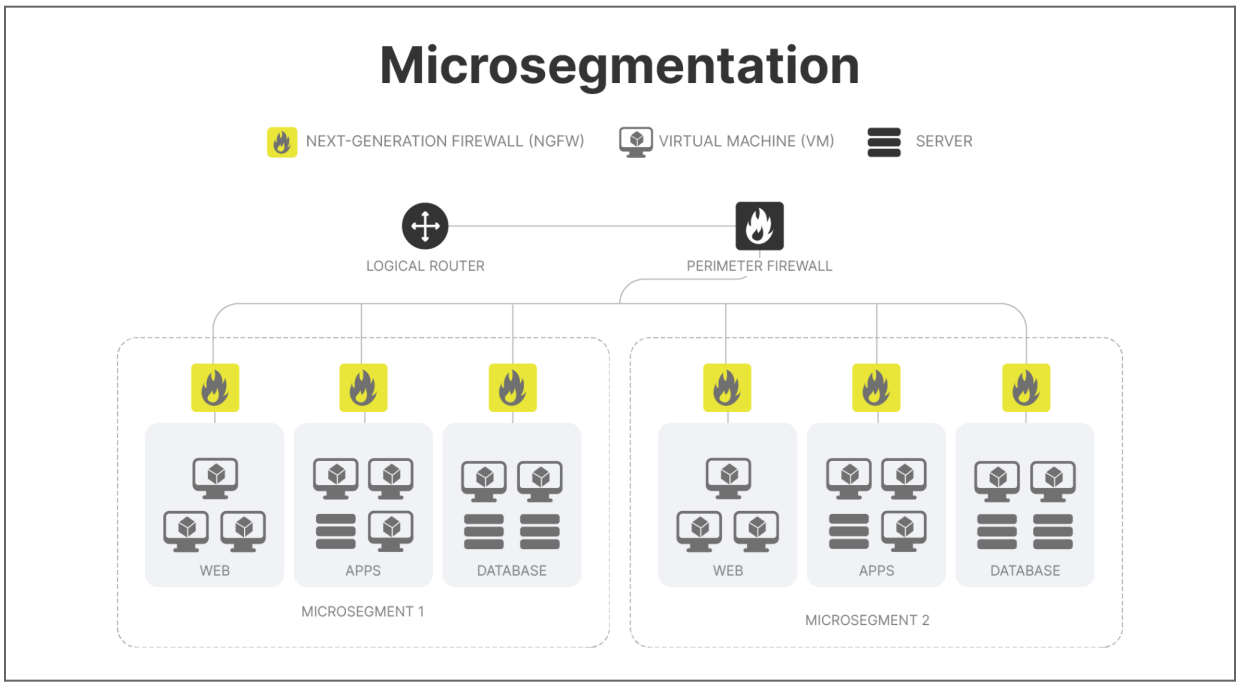
So once again, here is where the ZTF applies. Not only can it provide the attributes of both 2FA and MFA, but it also offers a multi-tiered approach so that the likelihood of a cybercriminal accessing a company's most sensitive data is drastically reduced, effectively impossible.

The Zero Trust Framework Approach

From a semantic standpoint, the best way to define the ZTF is through five core principles:

1. Security relies on the assumption that every single user is hostile
2. Threats, both internal and external, exist on the network at all times
3. Locality is not enough for deciding trust in a network
4. Every user and device should be authenticated and authorized
5. Policies must be dynamic and rely on many sources of data.

The ZTF (see Figure B below) does away completely with the notion of having just one, large Perimeter Security. Rather, the approach here is to take an entire schematic of the business, and break it down into smaller, more manageable units. Obviously, the one area that is



[Figure B] (Source: www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network)

going to come under heavy scrutinization is that of the IT and Network Infrastructure, due to it storing all of a company's digital assets within the servers, database, web applications, etc. Although they are all afforded some security through the use of 2FA and MFA, the traditional model here still falls under the realms of the Perimeter Security approach. But with the ZFT, a substantial paradigm shift has occurred. Each key area of the IT and Network infrastructure now becomes separated into their own islands, surrounded by their own layer of security. It is through this layer of security that an end user will have to present at three or more layers of authentication (for purposes of this journal article, we will assume that this is the type of MFA used).

For example, the email server, the database server, the web application server could all be their own islands. With the ZTF, digital assets are broken down into smaller units which are significantly more manageable to secure, known as 'microsegments'. An easy comparison for this process is the creation of different subnets in an entire Network Infrastructure, although in the ZTF scenario companies are subnetting out the various components of their digital assets with the MFA approach. The most distinct advantage with the ZFT is that it prevents the lateral movement, or in the worst-case scenario, greatly slows down the movement of the cybercriminal.

For example, the cybercriminal might be able to breach the first line of defense, but over time, their movements are halted as they continue to encounter additional authentication steps. This is a key tenet of the ZTF. While each island must have MFA, the authentication mechanisms used to confirm the identity of the end user (in the corporate setting, an employee, remote worker, or contractor) must all be different from one another. Types of authentication can include a password, an RSA Token, a Biometric modality (which helps to confirm an end user's identity based upon their unique physiological and/or behavioral features), smart cards and challenge/response questions.

Another key component of the ZTF is that individuals must be constantly verified because the concept of trust, as aforementioned, doesn't exist. For example, after access to one resource has been granted, the same sequence of authentication must be repeated to gain access to yet another shared resource. Naturally the pushback from corporate settings is that this repeated authentication process can prove to be

time consuming, leading to the concepts of Privileged Access Management (which is a subset of Identity and Access Management known as PAM) which can be implemented. Once the first set of at least three or more credentials have been identified and used, they can also be used in a different sequence to gain access to the next shared resource that also requires these credentials.

Another key advantage of the ZTF is that since different authentication mechanisms are being used, the total eradication of passwords is now theoretically possible. The essence of the ZTF can be derived from its slogan: “Never Trust, Always Verify”.

The Advantages of the Zero Trust Framework

1) ZTF facilitates the use of centralized monitoring:

   When security tools and technologies are used in conjunction with one another in an ill-planned manner, it can be very difficult for the IT Security team to track and respond in a timely fashion to the warnings and alerts. This creates difficulty in triaging and escalating the most serious cyber threats. With the Zero Trust methodology, since each device is accounted for in a logical manner, a centralized approach can now be utilized. One typical example of this is the Security Incident and Event Management software application. With this application, not only can the false positives be filtered out by making use of both Artificial Intelligence (AI) and Machine Learning (ML), but the legitimate warnings and alerts can be presented in a real-time basis through a centralized dashboard. Thus, ZTF allows the IT Security team to be far more proactive, and in turn, greatly reduce the response time in combating various threat vectors.

2) Scalability is offered:

   With an increasing number of companies employing remote workforces, many are now opting to make greater usage of Cloud-based resources, such as those offered by the AWS or Microsoft Azure. Certain entities still choose to have a brick-and-mortar presence and, consequently, still have some remnants of an On Premises solution. Regardless of the option chosen, the ZTF allows for the seamless transfer for apps, digital assets, and even the confidential information and data (especially the Personal Identifiable Information [PII] datasets) from one place to another in a secure and safe fashion.

3) Breaches become virtually impossible:

   Before the Covid-19 pandemic hit, many businesses adopted the “Perimeter Security” approach to protecting their digital assets, meaning there was only one line of defense separating the internal environment from the external environment. As a result, if the cybercriminal were to penetrate through this perimeter, they could gain access to just about anything in the IT and Network Infrastructure and move covertly through the organization, all the while accessing sensitive company information. But with the ZTF, the implementation of multiple layers of security means that it becomes that much harder for the cybercriminal to gain access to said information, as it will take significantly longer to break through every line of defense and easy for security teams to respond to said cybercriminal before the threat actor has accessed pertinent company data. In the end, the cybercriminal is likely to not see this particular endeavor as worth their time.

It is very important to note that the ZTF is not a product, nor does it take a one size fits all approach. Rather, it is deemed to be a methodology, of which the parts and components of it must be tailored to the security requirements of each individual entity. For example, although the ZTF explicitly states that each and every asset must be protected, commercial reality may dictate

otherwise. Low risk digital assets may not have to become their own island - indeed it may be acceptable to combine multiple assets in one island.

In the next section, some of the critical variables in deploying a comprehensive ZTF are examined.

Zero Trust Framework Implementation - Consideration Factors

When implementing ZTF for a company, here are some prominent considerations:

1) **Determine what needs to be protected:**

One of the fundamental concepts behind the ZTF is that an entire IT and Network infrastructure has to be broken out into different segments. Although the overall goal is to have a 100% breakdown, this may not be feasible, depending upon a company's security requirements. For this reason, companies should work with their IT Security teams and carefully map out what really needs to be protected, and how it can be further divided. It is important to note that this isn't a one-time, static analysis, but rather should aim to be dynamic and scalable. For example, if the IT/Network infrastructure grows or shrinks over time, the ZTF that is deployed should follow in tandem. A micro view is required beyond a macro view, since each layer of separation will require its own needs and attention. This kind of approach is also known as "DAAS", which stands for critical Data, Software Applications, Digital Assets and Services.

2) **Determine how data flows:**

Normally taken for granted, with ZTF how data flows within an IT/Network infrastructure must be carefully mapped. Since segmenting is occurring, there needs to be a clear and seamless flow for the data packets to avoid them being blocked off at one point and not being able to reach the other segment. This type of analysis yields a clearer picture of the controls that could potentially be needed, and how best they should fit into the model strategically.

3) Create a tentative model:

The next step is to actually formulate a working model of the ZTF. It is very important to keep in mind that at this stage, there is no one size fits all approach. A ZTF should be created according to individual security needs. At this stage, one of the key items to consider is the type of authentication mechanisms that will be needed, and where they should be placed so that they best support the controls that will be implemented. With this methodology, MFA is an absolute necessity, where at least three or more tools must be implemented in order to fully confirm the identity of an end user. Furthermore, they must also be different in nature, according to the following rules:

- Something you know;
- Something you have;
- Something you are.

For example, a password could be used for the first, an RSA token could be used for the second, and a Biometric could be used for the third. Meaning, the end user has to present all three pieces before they will be granted access to the shared resources. Another key item to remember is that each segment in the ZTF should not repeat the same authentication sequencing from the previous layer. To illustrate this, the second layer should consist of a set of challenge/response questions, a smart card which contains more detailed information about the end user, and a different Biometric modality. Finally if more than three authentication

mechanisms are implemented, a greater level of security is attained.

4) **Creating the policies:**

Another key element of the ZTF is the creation of the Security Policy acts as its foundation. It should at minimum, consist of the following to enforce yet another layer of security:

- Which end users should be accessing what resources;
- An audit log of the resources and applications that are being accessed;
- The times of the day in which shared resources can be accessed;
- Implementation of the Next Generation Firewall to allow even more advanced filtering and blocking of malicious data packets.

5) **Daily Monitoring:**

Once a working model of ZTF is created, it should then be deployed. However, avoid rolling this out all at once and instead use a phased approach. For example, rather than deploying all of the authentication mechanisms for each segment, do them one at a time. That way, if any unforeseen issues come up, they can be resolved in an efficient and manageable fashion.

Multi Factor Authentication in the Zero Trust Framework – The use of Biometrics

MFA is at the very heart of the ZTF. Because of the advancements that have been made in other forms of authentication technology, it is now possible to eradicate the Password in its entirety. If this will truly ever be done depends less on scientific reason and more upon human psychology. But the ultimate goal of this journal article is to lay down the foundation to turn this into an actual reality.

As discussed, there are the RSA tokens, smart cards, FOBs, challenge/answer response questions, etc. However, these still can be tampered with to varying degrees. Therefore, some other modality that is almost bulletproof for a malicious threat actor to tamper with must also be deployed. This is where Biometrics comes into play. There are three of them, and they are as follows:

1) Fingerprint Recognition;

2) Iris Recognition;

3) Facial Recognition.

A primary advantage of using these three is that they are proven, and are very durable in nature. Thus, they can fit into just about any type of ZTF environment that has been created. Finally, they are all non-contactless – which is a concern in a pandemic-sensitive world.

The Longest Known Biometric – Fingerprint Recognition

Fingerprint Recognition is the longest lasting biometric technology. The use of it dates back to the 1500's, becoming the de facto standard for law enforcement.

The details of the fingerprint are broken down into three distinct levels:

(1) Level 1: The pattern images which are present in the fingerprint;

(2) Level 2: The minutiae points of the fingerprint (this is from where the bulk of the unique features are actually extracted from);

(3) Level 3: The shapes and the images of the ridges, and its associated pores.

It is important to note at this point that biometric based fingerprint systems only collect images at Levels 1 and 2. Only the most powerful fingerprint recognition systems collect Level 3 details, used primarily for identification purposes. The Levels 1 & 2 specific features include the following:

(1) Arches: These are the ridges which just flow in one direction, without doubling back, or going backwards. These only

(2) comprise about 5% of the features of the fingerprint;

(3) Loops: These are the ridges that go backwards, and go from either left to right or vice versa. There are two distinct types of loops: a) Radial loops which angle downwards; and b) the ulnar loop which angle upwards These make up 65% of the features within the fingerprint;

(4) Whorls: The ridges in the fingerprint that make a circle around a core, and these comprise 30% of the features in the fingerprint.

The Process of Fingerprint Recognition

Fingerprint recognition follows a distinct methodology which can be broken down into the following steps:

(1) The actual, raw images of the fingerprint are acquired through the sensor technology, inclusive of a quality check. The raw images are examined by the biometric system to see if there is too much extraneous data in the fingerprint image, which could interfere in the acquisition of unique data. If there is too much of an obstruction found, the fingerprint device will automatically discard that particular image, and prompt the end user to place their finger into the platen for another raw image of the fingerprint to be collected. If the raw images are accepted, they are subsequently sent over to the processing unit, which is located within the fingerprint recognition device;

(2) With the raw images accepted by the system, the unique features are then extracted, and then stored as the enrollment template. If fingerprint recognition is being used by a

smartphone, a smart card is then utilized to store the actual enrollment template, and can even provide for some processing features for the smartphone;

(3) Once the end user wishes to gain physical or logical access, the user then has to place their finger onto the sensor of the fingerprint recognition system, so that the raw images and unique features can be extracted as described up above, and this becomes the enrollment template. The enrollment and verification templates are then compared to one another, to determine the degree of similarity/non-similarity with one another;

(4) If the enrollment and verification templates are deemed to be close in similarity, the end user is then verified and/or identified, and is then granted either the physical or logical access they are seeking.

The Matching Algorithm

As mentioned, it is the matching algorithm which compares the enrollment template with the verification template, and in order to ascertain the degree of similarity or closeness between the two, a certain methodology must be followed, described as follows:

(1) Whatever data is collected from the raw image of the fingerprint, it must have some sort of commonality with the enrollment biometric template which is already stored in the database. This intersection of data is known as the core, or the maximum curvature in a ridgeline.

(2) Any extraneous objects which could possibly interfere with the unique feature extraction process must be removed before the process of verification/identification can actually occur. Some of these extraneous objects can be the various differences found in the size, pressure, and the rotation angle of the fingerprint, and these can be normalized and removed by the matching algorithm.

(3) In the final stage, the unique features collected from the raw data (which become the verification template) must be compared to that of the enrollment template later. At this stage, the matching algorithm does the bulk of its work, based upon the premise of three types and kinds of correlations:

(a) **Correlation Based Matching:** When two fingerprints are superimposed, differences at the pixel level are calculated. Although it is strived for, perfect alignment of the superimposed fingerprint images is nearly impossible to achieve. A notable disadvantage with this correlation method is that performing these types of calculations can be very intensive from a processing perspective, which can be a great strain on computing resources.

(b) **Minutiae based matching:** In fingerprint recognition, this is the most widely used type of matching algorithm. With this method, it is the distances and the angles between the minutiae which are calculated and subsequently compared with another. There is global minutiae matching as well as local minutiae matching, and the latter method focuses upon the examination of a central minutiae, as well as the nearest two neighboring minutiae.

(c) **Ridge Feature Matching:** With this matching method, the minutiae of the fingerprint are combined with other finger-based features such as shape and size, the number and the position of various singularities, as well global and local textures. This technique is especially useful if the raw image of the fingerprint is poor in quality, and these extra features can help compensate for that deficit.

It should be noted that with all Biometric modalities, the raw templates that are collected are never stored permanently in the database of the system that is being used. Rather they all get converted over into a mathematical file or a statistical profile for comparison purposes between the enrollment and verification templates. With regards to Fingerprint Recognition, the raw images are converted into a binary mathematical file, such as the example that follows:

00011111000111100001110000O

This is what makes Biometric modalities almost hack proof: What can a cybercriminal do with a binary mathematical format? It's not the same as stealing a credit card number.

The Most Stable Biometric – Iris Recognition

The iris lies between the pupil and the white of the eye, which is known as the sclera. The color of the iris varies from individual to individual, but there is a commonality to the colors, and these include green, blue, brown, hazel, and, in the most extreme cases, a combination of these colors. The color of the iris is primarily determined by the DNA code inherited from our parents.

The unique pattern of the iris starts to form when the human embryo is conceived, usually during the third month of fetal gestation. The phenotype of the iris is shaped and formed in a process known as chaotic morphogenesis, and the unique structures of the iris are completely formed during the first two years of child development.

The primary purpose of the iris is to control the diameter and the size of the pupil. The pupil is that part of the eye which allows for light to enter into the eye, which in turn reaches the retina, which is located in the back of the eye.

Of course, the amount of light which can enter the pupil is a direct function of how much it can expand and contract, which is governed by the muscles of the iris. The iris is primarily composed of two layers: (1) A fibrovascular tissue known as

the stroma, and (2) the sphincter muscles, a group of muscles that connects to the stroma.

Sphincter muscles are responsible for the contraction of the pupil, and the dilator muscles govern the expansion of the pupil. Observing an iris in the mirror, one notices a radiating pattern, called the trabecular meshwork. When Near Infrared Light (NIR) is flashed onto the iris, many unique features can be observed. These features include ridges, folds, freckles, furrows, arches, crypts, coronas, as well as other patterns which appear in various, discernable fashions.

Finally, the collaretta of the iris is the thickest region of it, also containing unique features, which gives the iris its two distinct regions, known as the pupillary zone (this forms the boundary of the pupil), and the ciliary zone (which fills up the rest of the iris). The iris is deemed to be one of the most unique structures of human physiology, and in fact, each individual has a different iris structure in both eyes. Scientific studies have shown that even identical twins have different iris structures.

The Algorithms – Iris Codes

The idea of using the iris to confirm an individual's identity dates back to 1936, when an ophthalmologist, Frank Burch, first proposed the idea. This idea was then patented in 1987, and by the mid-nineties, Dr. John Daugmann of the University of Cambridge developed the first mathematical algorithms for it.

Traditional iris recognition technology requires that the end user stand no more than ten inches away from the camera. With the NIR light shined into the iris, various grayscale images are then captured, and then compiled into one primary composite photograph. Software then removes any obstructions from the iris, which can include portions of the pupil, eyelashes, eyelids, and any resulting glare from the iris camera.

From this composite image, the unique features of the iris (as described before) are then "zoned off" into hundreds of phasors (also known as vectors), whose measurements and amplitude level are then extracted (using Gabor Wavelet mathematics), and then subsequently converted into a small binary mathematical file, no greater than 500 bytes. Because of this very small template size, verification of an individual can occur in just less than one second.

In traditional iris recognition methods, this mathematical file then becomes the actual iris biometric template, which is also known as the "IrisCode". However, in order to positively verify or identify an individual from the database, these iris-based enrollment and verification templates (the IrisCode) must be first compared with one another. In order to accomplish this task, the IrisCodes are compared against one another byte by byte, looking for any dissimilarities amongst the string of binary digits.

In other words, to what extent do the zeroes and ones in the iris-based enrollment and verification templates match up against one another? The answer is found by using a technique known as "Hamming Distances", which is still used in modern iris recognition algorithms.

After these distances are measured, tests of statistical independence are then carried out, using high level Boolean mathematics (such as Exclusive OR Operators [XOR] and Masked Operators). Finally, if the test of statistical independence is passed, the individual is then positively verified or identified, but if the tests of statistical independence are failed, then the person is NOT positively verified or identified.

The Most Controversial Biometric – Facial Recognition

Facial recognition technology relies upon the physical features of the face of which are determined by genetics. Also, this technology can either be deployed either as a fully automated system, or as a semi-automated system. With the latter, no human interaction is needed, all of the verification and identification decisions are made by the technology itself. With the latter, human intervention to a certain degree is required, and this is actually the preferred method for deploying a facial recognition system.

Facial recognition systems focus upon those parts of the face which are not as easily prone to obstacles. These facial regions that are collected for a raw sample include the following:

(1) The ridges between the eyebrows;

(2) The cheekbones;

(3) The mouth edges;

(4) The distances between the eyes;

(5) The width of the nose;

(6) The contour and the profile of the jawline;

(7) The chin.

The methodology to capture the raw images of the face differs substantially to the other Biometric technologies. Although facial recognition is a non-contactless technology, the image capture process is significantly more complex, and more cooperation is required on part of the end user. To start the process of raw image collection, the individual must first either stand before a camera, or unknowingly, have their face captured with covert surveillance methods, such as using a CCTV camera system.

Once the raw images are collected by the camera, the data is then either aligned or normalized to help refine the raw images at a granular level. The refinement techniques involved include adjusting the face to be in the middle of the pictures which have been taken, and adjusting the size and the angle of the face so that the best unique features can be extracted and later converted over to the appropriate verification and enrollment templates.

All of this is done via mathematical algorithms. As mentioned previously, facial recognition is countered by a number of major obstacles, but even more so at the raw image acquisition phase. These include a lack of subtle differentiation between the faces and other obstructive variables in the external environment, various different facial expressions and poses in subsequent raw image captures, and capturing a landmark orienting feature such as the eyes.

To help compensate for these obstacles, substantial research and development has been done in the area of 3-Dimensional imaging. In this

technique, a shape is formed and created, and using an existing 2-Dimensional image, various features are created, resulting in a model which can be applied to any 3-Dimensional surface and used to help compensate for the above-mentioned differences.

However, it should be noted that these types of 3-Dimensional facial recognition systems are not widely deployed in commercial applications yet, because this technique is still pending further research. Right now, 2-Dimensional facial recognition systems are primarily used in the commercial market. 3-Dimensional facial recognition systems are only used as a complement to the 2-Dimensional ones, in which higher imaging requirements are dictated, and the capture environment is much more challenging.

The Techniques of Facial Recognition

To help alleviate these obstacles and to provide a solution in which a single facial image can be detected in just one frame, various techniques have been developed and applied to facial recognition. These techniques fall under two categories:

(1) Appearance based;

(2) Model based.

With appearance based facial recognition techniques, a face can be represented in several object views, and it is based on one image only with no 3-Dimensional models used. The specific methodologies here include Principal Component Analysis, and Linear Discriminant Analysis. Model based facial recognition techniques construct and create a 3-Dimensional model of the human face, and subsequently, the facial variations can be captured and computed. The specific methodology here includes Elastic Bunch Graph Mapping.

Principal Component Analysis (this is linear based, also known as PCA) dates back to 1988, when it was first used for facial recognition. This technique primarily uses what is known as “Eigenfaces”. Simply put, Eigenfaces are just merely 2-Dimensional spectral facial images, which are composed of grayscale features.

There are literally hundreds of Eigenfaces which can be stored in the database of a facial recognition system. When facial images are collected by the system, this library of Eigenfaces is superimposed over the raw images. At this point, the level of variances between the Eigenfaces and the raw images are then subsequently computed, averaged together, and then different weights are assigned.

The end result is a 1-Dimensional image of the face, which is then processed by the facial recognition system. In terms of mathematics, PCA is merely a linear transformation in which the facial raw images get converted over into a geometrical coordinate system. Imagine a quadrant-based system. With the PCA technique, the data set with the greatest variance lies upon the first coordinate of the quadrant system (this is also termed the first PCA), the next data set with the second largest variance falls onto the second coordinate, and so on, until the 1-Dimensional face is created.

The biggest disadvantages with this technique are that it requires a full-frontal image, and as a result, a full image of the face is required. Thus, any changes in any facial feature requires a full recalculation of the entire Eigenface process. However, a refined approach has been developed, thus greatly reducing the calculating and processing time which is required.

Linear Discriminant Analysis (this is linear based, also known as LDA) projects the face onto a vector space, with the primary objective being to speed up the verification and identification processes by cutting down drastically on the total number of features which need to be matched.

The mathematics behind LDA is to calculate the variations which occur between a single raw data point from a single raw data record. Based on these calculations, the linear relationships are then extrapolated and formulated. One of the advantages of the LDA technique is that it can actually take into account the lighting differences and the various types of facial expressions which can occur, however a full-face image is still required.

After the linear relationship is drawn from the variance calculations, the pixel values are captured, and statistically plotted. The result is a computed raw image, called a Fisher Face, which is just simply a linear relationship of the various pixel values. Despite the advantages, a major drawback of the LDA technique is that it does require a large database.

Elastic Bunch Graph Matching (this is model based, also known as EBGM) looks at the nonlinear mathematical relationships of the face, which includes factors like lighting differences, and the differences in the facial poses and expressions. This technique uses a similar technique which is used in iris recognition, known as Gabor Wavelet Mathematics.

With the EBGM technique, a facial map is created. The facial image on the map is just a sequencing of graphs, with various nodes located at the landmark features of the face, which include the eyes, edges of the lips, tips of the nose, etc. These edge features become 2-Dimensional distance vectors, and during the identification and verification processes, various Gabor mathematical filters are used to measure and calculate the variances of each node on the facial image.

Then, Gabor mathematical wavelets are used to capture up to five spatial frequencies, and up to eight different facial orientations. Although the EBGM technique does not require a full facial image, the main drawback with this technique is that the landmarks of the facial map must be marked extremely accurately.

How Biometric Modalities into the ZTF

So, we have now reviewed at length three distinct Biometric modalities that can now fit into the MFA model for the ZTF (remember, MFA was previously defined as having at least three or more layers of unique authentication mechanisms). Remember, all of the templates (both verification and enrollment) that have been created are some type of mathematical or statistical profile. The following matrix summarizes this:

Biometric Modality	***Outputted Mathematical File***
Fingerprint Recognition	Binary Digits
Iris Recognition	Iris Codes, based upon Gabor Wavelets
Facial Recognition	Eigenfaces, based upon Hidden Markov Models

At this point in time, these three Biometric modalities can literally fit anywhere into the ZTF infrastructure that have been deployed. They can be used at the beginning stages, or even in the middle of the Microsegments that have been broken out. Take for example a mid-level employee, such as that of a Database Administrator. This particular individual will probably have the most interest in gaining access to one (or perhaps) more of the databases at the organization.

But before this can happen, they first must be authenticated. This can be done by a rapid-fire succession of these three modalities. Although the exact time to elapse here has not been calculated, it has been estimated that it should take no more than three minutes as these are all non-contactless technologies. This is the point where all of the verification templates will be created, and compared against the enrollment templates. This part of the ZTF can be referred to as the “Point of Authentication”.

From here, the results of the authentication process will then be transferred to the lines of defense surrounding the database (whichever one the administrator wishes to access), to allow for the authorization of the shared resources to occur.

This can be referred to as the “Point of Authorization”. In this example, it has also been assumed that the principles of PAM will be followed. Because of this, there will be no need for this individual to have to go through the entire verification process across all of the three different modalities, because the results will have already been stored in the PAM Vault Box.

If access is needed to any of the other sub directories or sub shared resources in this

database, the same results will also apply. The only time when this individual will have to repeat the verification scenario just described is if they need to gain access to a different server, such as an Email server. This entire process can be seen in Figure C below.

As it was also described earlier in this journal article, it is only the enrollment template that is actually stored into the database of any of these three Biometric modalities and even then they are simply mathematical and/or statistical files. Thus, even if a cybercriminal were to breach a company's systems and hijack these templates, there is really nothing useful that can be done with them, as it requires a live sample for any level of authorization to take place.

This means that despite all of the lines of defenses offered up by the ZTF, there is still a potential vulnerability. Of course this needs to be remediated with the right controls, but if the templates are also in any danger of being hijacked, then it is also best to protect them as well. This is where they can be encrypted via BioCryptography as a further way to fortify the overall ZTF.

A Brief Review Into Bio Cryptography

The Cipher Biometric Template

When the fingerprint/iris/facial template is encrypted, it can be viewed as the "Cipher Biometric Template", and when it is decrypted, it can be viewed once again as the decrypted "Plaintext Biometric Template". Besides this, Bio Cryptography also has to provide the following three functions in order for it to be truly effective:

1) **Authentication:** The receiver of the message (or the Plaintext Biometric Template) should be able to accurately verify the origin of it;
2) **Integrity:** The message in transit (or the Plaintext Biometric Template) should not be modified in any way or format while it is in transit (or in other words, replacing a fingerprint biometric template with an iris biometric template in order to spoof the biometric system). This is where Quantum Cryptography can contribute heavily, making use of particle photons and their polar angles.
3) **Nonrepudiation:** The sender of the Plaintext Biometric Template should not falsely deny that they have not sent that particular template originally.

Biocryptography Keys

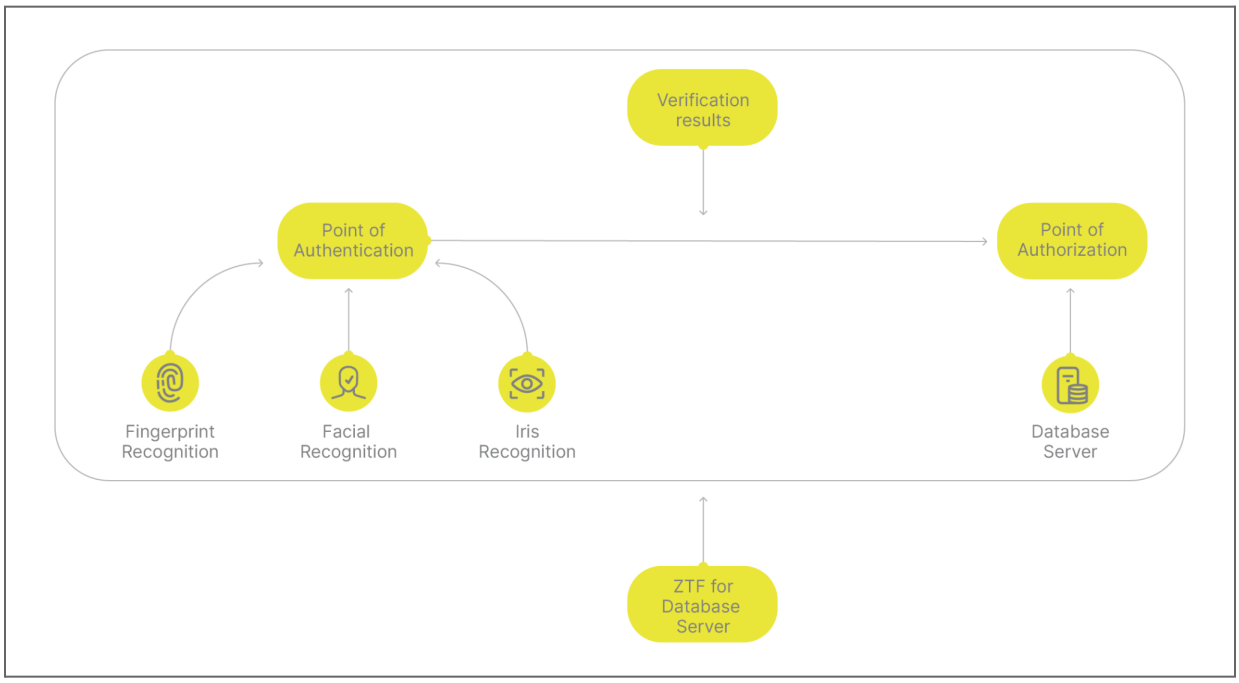
A component which is central to Bio Cryptography are what is known as "keys". It is the key itself which is used to lock up the Plaintext Biometric Template (or encrypt it) at the point of origination, and it is also used to unlock that same Template at the receiving end.

The key itself is a series of mathematical values - the larger the value, the harder it is to break while it is in transit. The range of possible mathematical values is referred to as the "keyspace".

There are many types of such keys used in Bio Cryptography, such as signing keys, authentication keys, data encryption keys, session keys, etc. The number of keys which are generated depends primarily upon the mathematical algorithms which are used, grouped into either symmetric and asymmetric.

To further fortify the strengths of a Bio Cryptography-based Public Key Infrastructure, mathematical hashing functions are also used to protect the integrity of the Plaintext Biometric Template. For example, when the destination party receives the Plaintext Biometric Template, the hashing function is included with it.

If the values within the hashing function have not changed after it has been computed by the



[FIGURE C]

receiving end, then one can be assured that the Plaintext Biometric Template has not been changed or altered in any way.

To prove the validity of the hashing functions, it should be noted that they can be calculated only in one direction (e.g. going from the sending point to the receiving point, where it is computed), but not in the other direction (e.g. going from the destination point to the origination point).

The hashing function will be reviewed again in the next section of this journal article. It should be noted that for purposes of this study, the ZTF methodology that we have introduced is rather simple in nature, as we have focused on solely one segment of it – namely a Database Server. So therefore, one can assume that for illustrative purposes, Symmetric Key Cryptography is used. This is where one secret key, namely the Private Key, will be used to encrypt and decrypt the template.

There are inherent risks using this approach, especially if the Private Key is given out to another party. But with the safety mechanisms already afforded by the ZTF, and the mathematical nature of the templates, this should help offset this risk. But as the ZTF gets deployed into the real world on a grander scale, it is quite conceivable that Asymmetric Key Cryptography will have to be used, which uses a combination of both Public and Private Keys, and even a Key Distribution Center (KDC).

Also, only one biometric template will truly need to be encrypted, which is the enrollment template. As described previously, this is what gets stored in the database of the biometric device, and is used to confirm the authenticity of an individual.

In fact the concepts of BioCryptography were first explored on a major basis by Ravi Das in his book: "Biometric Technology: Authentication, BioCryptography, and Cloud Based Architecture", published by CRC Press in 2015.

Conclusion - Other Factors For MFA In The ZTF

What we have proposed is a ZTF making key usage of biometrics in a full effort to eradicate the use of passwords altogether. But also as mentioned, there are other mechanisms that can be used - such as RSA tokens, smart cards, etc. Although we have outlined earlier the steps that

need to be taken to have an effective ZTF methodology, there are some other factors relating to MFA that must be taken into consideration as well, specifically adaptive MFA. The decision if MFA needs to be applied at a specific time, for a specific user will depend on policies that can be static or dynamic.

Adaptative MFA is based on the simultaneous analysis of many data points (IP, location, time, device, etc). Adaptative MFA will require authentication requirements based on the following criteria:

- **Static Policies:** risk levels are defined based on different data points.
- **Dynamic Policies:** policies change based on the analysis of users' behavior. In this case, Machine Learning techniques can be used to optimize policies and reduce risk over time.
- **Hybrid:** A combination of static and dynamic policies.