ZTF: The Secret to a Seamless Authentication Experience

By Ravi Das, Anthony Figueroa, and Patrick Ward

Contents

CHAPTER 1: INTRODUCTION

In today's world, where cyberattacks are becoming increasingly sophisticated, businesses and organizations need to take steps to secure their networks and protect sensitive information. The future threats to our companies, communities, and countries will not come from the physical world, but rather, will come from the virtual realm.

To safeguard against these threats, the approaches to security of the past are insufficient and new approaches must be developed. One approach to achieving this higher level of protection is the zero-trust security framework, which assumes that all devices and users on a network are potentially compromised and must be verified and authorized before being granted access to resources. The goal of this book is simple: to provide a comprehensive overview of how to implement a zero-trust security framework and the corresponding role of biometrics in said framework.

The use of biometric authentication is an essential aspect of a zero-trust security strategy. Biometrics use physical characteristics to identify individuals, such as fingerprints, facial features, or iris scans. This type of authentication provides an added layer of security compared to traditional password-based authentication, which can be easily compromised or shared among multiple users.

Biometric authentication is essential in implementing a zero-trust security framework. Password-based authentication, which is commonly used, can be compromised or shared among multiple users, making it less secure. Biometric authentication, on the other hand, provides an added layer of security by using physical characteristics to identify individuals, making it difficult to duplicate or replicate.

Benefits of using biometric authentication include enhancing security, detecting anomalies in user activity, and preventing unauthorized access to sensitive resources. It is also worth mentioning and emphasizing the need for careful consideration when implementing biometric technology, including choosing the right type of biometric technology, ensuring compliance with privacy and data protection regulations, and ensuring that biometric data is stored and processed securely.

When dealing with biometric data and its corresponding authentication, it is vital to consider the role of privacy and data protection. Biometric data is highly personal and sensitive, and it is crucial to ensure that it is stored and processed securely and in compliance with applicable privacy regulations.

Various privacy laws and regulations, such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Biometric Information Privacy Act (BIPA) in Illinois, apply with respect to the handling of personal private information and data. It is imperative for businesses to be transparent about how they collect, store, and use biometric data and obtain explicit consent from users.

We must remember, in spite of the advantages of biometric authentication, there are several challenges and limitations of biometric technology in a zero-trust security framework. While biometrics provide an added layer of security, they are not foolproof and can be vulnerable to spoofing or other attacks. Common types of biometric attacks, such as presentation attacks and replay attacks, do exist and it's important to have a contingency plan in place for situations where biometric authentication fails, such as providing alternative authentication methods or temporarily suspending access to sensitive resources. All

forms of security are not 100 percent guaranteed so tread with caution - no security solution is a silver bullet.

Indeed, when you combine forms of authentication through multiple forms of security, as is the case in multi-factor authentication (MFA), the use of biometrics can make your solution even more secure. MFA combines multiple forms of authentication, including biometrics, to significantly increase security and reduce the risk of unauthorized access.

Needless to say, the main benefits of MFA are enhanced security, reduced risk of account takeover, and improved compliance with regulatory requirements. It is also worth appreciating the various types of MFA, including knowledge-based authentication (KBA), possession-based authentication, and inherence-based authentication (biometrics). One must use careful consideration when implementing MFA, including assessing the level of risk, choosing the right combination of authentication methods, and ensuring ease of use for users.

There are many benefits and challenges of implementing biometric technology in a zero-trust security framework. Careful planning and consideration is critical when implementing biometric technology, including choosing the right type of biometric technology, ensuring compliance with relevant regulations, and developing clear policies and procedures for handling biometric data.

For every upside, however, there is a downside and challenges do exist in the management and maintenance of biometric data, such as data accuracy, data quality, and data retention. One way to mitigate these challenges is by having clear policies and procedures in place to ensure that biometric data is handled securely and responsibly. Also, remember that policies aren't a 'set it and forget it' strategy - you need to be vigilant in training and educating users on how to use biometric authentication and ensuring that users are comfortable with the technology.

There is always a need for ongoing monitoring and assessment of the biometric authentication system to ensure that it remains effective and compliant over time.

We hope this book will be a valuable resource for businesses and organizations looking to implement a zero-trust security framework. We hope you gain a detailed overview of the role of biometrics in a zero-trust security strategy, understand the challenges and limitations of biometric technology, and place a great deal of importance on privacy and data protection.

Our goal is for you to reap the benefits of multi-factor authentication and use practical guidance on how to implement biometric technology effectively and compliantly.

CHAPTER 2 – A Review Of Cryptography

Introduction

In this chapter we are going to review some fundamental concepts that are key to understanding cryptography, as well as review the most ancient sources of information that we know have used one way of cryptography.

A Brief History. From Ancient Times To Modernity

On its most basic level, people have historically tried to establish secure lines of communication between parties. This is true and desirable today, when chatting with a friend, but also centuries ago when secret communication had to be manually transported over hundreds of miles. In these cases, a man-in-the-middle attack could carry a more literal connotation and exposure of information could be as straightforward as reading a sheet of paper.

Cryptography has been used for thousands of years to protect information from unauthorized access and manipulation. The simplest forms of cryptography were substitution ciphers used in ancient times, and it has had an uneven evolution throughout history until today's modern public key cryptography and more. Its history is rich and varied. This chapter will start with a brief overview of the history of cryptography, starting with ancient civilizations and continuing to modern times.

One of the earliest known uses of cryptography is in ancient Egypt, where hieroglyphics were used to protect information. The use of hieroglyphics allowed the ancient Egyptians to keep their information secure from outsiders and to prevent unauthorized access to sensitive information.

Hieroglyphics, meaning 'sacred carving' were a complex writing system that used over 700 different symbols to represent words, ideas, and even sounds. Symbols could be combined to create messages, but without a key to interpret these symbols, the messages would be indecipherable. This made the use of hieroglyphics an effective form of cryptography for ancient Egypt.

It is believed that only a select few individuals, such as scribes and priests, were trained to read and write in hieroglyphics. This exclusivity helped to maintain the security of the encoded messages, as it would have been difficult for an outsider to intercept and interpret the information. It would also have been difficult for a person not belonging to the elites to understand this mysterious art of communication. The encoding of messages in symbols served as an effective form of cryptography, ensuring that sensitive information was kept secure and inaccessible to those without the proper training and knowledge.

They were also very resistant to time since many people throughout the world tried in vain to decipher its writings. The key to decipherment was discovered in 1799: the Rosetta Stone. During the French occupation of Egypt, French soldiers who were repairing a fort in the port city of Rashid found a large broken stone from its foundations. On the stone were carved three distinct scripts: hieroglyphic, demotic and Greek. Prints and different versions of the Rosetta Stone were distributed across Europe. French scholar Jean-François Champollion and England's Thomas Young, working in parallel but without

knowledge of each other, realized that some of the hieroglyphs represented spoken words. On 14 September 1822, Champollion excitedly visited his brother. Champollion notes formed the basis of a historic letter in which Champollion outlined his findings on the translation of the hieroglyphs into royal names. This public reading of this letter was known as the moment of decipherment.

Taking a detour to classic times, in ancient Greece, the scytale, a rod used to encrypt messages by wrapping them around it, was widely used. It was a cylinder with a strip of parchment wound around it, on which a message was written in such a way that it could only be read when unwound from the rod.

The scytale was used as a cryptographic tool by the Spartans, who were known for their military prowess and secrecy. The message was written lengthwise along the strip of parchment and then wrapped around the rod. When the strip was unwound from the rod, the message appeared as a series of letters arranged in a seemingly random order, making it unreadable to anyone who intercepted it. To read the message, the recipient had to have a rod of the same diameter as the sender's, which was the only way to reorder the letters into their original sequence.

The use of a scytale ensured that the message would be secure, as the rod was typically kept by the sender and only given to the recipient when the message was to be read. This made it difficult for anyone who intercepted the strip of parchment to read the message, as they would not have access to the rod required to decode it. Additionally, the use of a scytale ensured that the message was tamper-proof, as unwinding the parchment from the rod would have caused the message to be destroyed.

The scytale was a simple but effective way to ensure the security of a message. It allowed the Spartans to send sensitive information without the risk of it falling into the wrong hands. While the scytale was a physical device and therefore limited in its use, it remains an interesting example of early cryptography and the lengths people have gone to in order to secure their communication.

Julius Caesar used a simple substitution cipher, known as the Caesar cipher, to protect messages sent to his military commanders. This cipher is one of the simplest and most widely known encryption techniques, and the first one that any student will learn in a cryptography course. It is a type of substitution cipher in which each letter in the plaintext is shifted a certain number of places down the alphabet. The number of positions shifted is referred to as the "key".

To decrypt a message encrypted with the Caesar cipher, the process is simply reversed. Each letter is shifted back a fixed number of places up the alphabet, again determined by the key. For example, consider the plaintext message "HELLO". Using a key of 3, the encrypted message would be "KHOOR". To decrypt the message, the reverse process is used, with each letter shifted back 3 places up the alphabet, resulting in the original plaintext message "HELLO".

The Caesar cipher is a simple but effective encryption technique that has a long history of use. No real use of this cipher can be used in modern day information technology, but despite its simplicity, the Caesar cipher is still widely used as an educational tool to teach the basics of cryptography, and it serves as an example of how encryption can be used to protect information.

During the Middle Ages, various other forms of substitution ciphers were used by various armies and monarchs to protect sensitive information. The invention of the printing press in the 15th century made it easier to distribute cryptographic methods, and various books on cryptography were published during this time. As wars, political unrest, and religious conflicts spread throughout Europe, the need for secure

communication became increasingly important. Monarchs and other powerful figures relied on cryptography to send secret messages and protect sensitive information.

Other simple, but effective for the times it was used, ways of ciphers started to arise, such as transposition ciphers, and polyalphabetic ciphers. Transposition ciphers involved rearranging the order of the letters in plaintext, while polyalphabetic ciphers used multiple alphabets to encrypt the same message.

One of the most famous examples of cryptography during the Middle Ages is the use of the Vigenère cipher. This cipher was first described by Giovan Battista Bellaso in 1553 and later improved by Blaise de Vigenère in the 16th century. The Vigenère cipher uses a repeating keyword to encrypt the message, making it much more secure than the simple substitution ciphers of the time.

With the widespread information during this time, not only were cipher methods well known, but people started to find methods to break ciphers. This led to the publication of numerous books on cryptography, including works by Johannes Trithemius, Girolamo Cardano, and others.

One notable book on cryptography published after the invention of the printing press is "Polygraphiae" by Johannes Trithemius, published in 1518. In this work, Trithemius discussed various forms of cryptography, including substitution ciphers and transposition ciphers. He also described the use of "steganography", which involves hiding a message within an innocent-looking cover text.

Another important and iconic book on cryptography is "De Furtivis Literarum Notis" by Girolamo Cardano, published in late 1550. This work described various forms of cryptography, including the use of substitution ciphers and transposition ciphers, as well as the invention of a new cipher known as the "Cardan grille".

It is a method of writing secret messages using a grid, which ends up being the key to the cipher. The main idea is to hide messages inside an ordinary letter so that the whole would not appear to be a cipher at all.

Today, many of these historical works on cryptography remain relevant, and continue to be studied and used as sources of inspiration for modern cryptographic techniques.

One of the most important developments in the history of cryptography occurred in the 20th century, with the invention of computer-based cryptography. With the advent of computers, encryption algorithms could be made more complex and secure, making it much more difficult for unauthorized users to access encrypted information.

The invention of public key cryptography in the 1970s was a major turning point in the history of cryptography. This new method of encryption allowed for secure communication without the need for a shared secret key. Public key cryptography works by using two keys, a public key used to encrypt the message and a private key used to decrypt the message. This makes it much easier to securely communicate over long distances, as the public key can be freely shared without compromising the security of the encrypted information.

Public key cryptography is a type of cryptography that uses two different keys, one for encryption and another for decryption. This allows for secure communication between two parties, without the need

for a shared secret key beforehand. We will discuss this method more deeply in **Chapter 4**, but in this chapter, we will provide a very simple example.

Let's consider the example of Bob and Alice who want to communicate securely over the internet. In traditional cryptography, Bob and Alice would need to share a secret key beforehand in order to encrypt and decrypt messages between them. However, in public key cryptography, Bob and Alice each have two keys: a public key and a private key.

Bob's public key is used to encrypt messages that are sent to him, and his private key is used to decrypt those messages. Similarly, Alice's public key is used to encrypt messages that she sends to Bob, and her private key is used to decrypt messages that she receives from Bob.

Here's how the process works:

Bob generates a pair of public and private keys. He then makes his public key publicly available, for example by publishing it on a key server.

Alice wants to send a message to Bob, so she retrieves Bob's public key and uses it to encrypt her message. The encrypted message can only be decrypted with Bob's private key.

Alice sends the encrypted message to Bob, and Bob uses his private key to decrypt it.

If Bob wants to send a reply, he uses Alice's public key to encrypt his message and sends it back to her.

It's important to note that the public key is used for encryption and the private key is used for decryption, and that the two keys are mathematically related but not the same. This means that anyone can use Bob's public key to encrypt messages for him, but only Bob has the private key that can be used to decrypt them.

One of the main benefits of public key cryptography is that it eliminates the need for a shared secret key beforehand. This makes it possible for two parties to communicate securely without having met in person or exchanged a secret key beforehand.

Another benefit is that public key cryptography can be used for digital signatures, which can be used to verify the authenticity of a message. In this case, the sender would use their private key to sign a message, and the recipient could use the sender's public key to verify the signature and ensure that the message came from the sender and was not tampered with during transit.

Public key cryptography is widely used for secure communication and has become an essential part of modern society. It is used for secure email communication, secure financial transactions, and secure data transfer, among many other applications.

With its ability to eliminate the need for a shared secret key beforehand, public key cryptography makes it possible for two parties to communicate securely without having met in person. This has enabled secure communication and transactions over the internet, making it an essential part of modern society.

In recent years, cryptography has become an increasingly important part of our daily lives, as we rely on it to protect sensitive information, such as financial transactions, personal data, and sensitive communications. The growth of the internet has made cryptography even more important, as it allows us to communicate and transfer information over long distances with relative ease.

The history of cryptography is a long and fascinating one, spanning thousands of years and covering a wide range of techniques and methods. From simple substitution ciphers used in ancient times to modern public key cryptography, cryptography has been used to protect information and facilitate secure communication throughout human history. With the continued growth of technology, cryptography will likely play an even more important role in our daily lives in the future.

Evolution: Substitution Ciphers to Public Key Cryptography

As technology advanced, more complex cryptographic techniques were developed. During World War II, for example, the Germans used the Enigma machine, a sophisticated electro-mechanical cipher machine, to encrypt messages. This machine was eventually broken by Allied codebreakers, leading to some of the most important victories of the war.

In the 1970s, a major breakthrough occurred in the field of cryptography with the invention of public key cryptography, as pointed out before. It is also known as asymmetric key cryptography. It allows for secure communication without the need for a shared secret key. This is achieved by using two keys, a public key used to encrypt the message, and a private key used to decrypt the message. This makes it much easier to securely communicate over long distances, as the public key can be freely shared without compromising the security of the encrypted information.

In Symmetric Key Cryptography, the same key is used for both encryption and decryption of the message. In this form of cryptography, both parties (sender and receiver) must have a shared secret key that they both know and use to encrypt and decrypt the messages they exchange.

This method of cryptography is fast and efficient, making it suitable for encrypting large amounts of data. However, the main drawback of symmetric key cryptography is that the shared key must be kept secret, and if the key is compromised, the security of the entire communication is at risk.

One of the main advantages of Asymmetric Key Cryptography over Symmetric Key Cryptography is that it provides authentication and confidentiality. By encrypting a message using a recipient's public key, the sender can be sure that only the intended recipient can decrypt it. Furthermore, the recipient can be sure that the message came from the sender, as only they would have access to the private key needed to encrypt the message.

Asymmetric Key Cryptography is often used in combination with symmetric key cryptography. For example, a session key can be securely exchanged using asymmetric cryptography, and then used for encrypting the data using symmetric cryptography, resulting in increased security and efficiency.

Another important development in the field of cryptography has been the invention of various encryption algorithms, such as the Advanced Encryption Standard (AES), the RSA algorithm and ECC. These algorithms are designed to be computationally infeasible to break, even with the use of the most powerful computers.

Some early examples of algorithms might be interesting and can bring some clarity around some topics. Some examples are AES, RSA and ECC

AES, which stands for Advanced Encryption Standard, is a symmetric key encryption algorithm that operates on fixed-size blocks of data of 128-bits. It uses the same key for encryption and decryption. It

also uses a combination of substitution and permutation operations, along with key expansion, to encrypt and decrypt the data. AES is widely used for encryption of sensitive data and is considered a strong encryption algorithm.

RSA (Rivest–Shamir–Adleman) is an asymmetric key encryption algorithm that uses two keys: a public key for encryption and a private key for decryption. RSA works on the mathematical property that it is easy to multiply two prime numbers but difficult to factorize their product. The security of RSA relies on the difficulty of factoring large numbers. RSA is widely used for secure data transmission, digital signatures, and key exchange.

In summary, AES is a fast and secure symmetric encryption algorithm, while RSA is a slower but more secure asymmetric encryption algorithm.

ECC, which stands for Elliptic Curve Cryptography, is a type of public key cryptography that uses the mathematics of elliptic curves over finite fields to provide security. ECC is considered to be more secure than other public key algorithms such as RSA, and is widely used for applications that require high security, such as digital signatures, key agreement, and encryption.

In this algorithm, a key pair is generated using a private key and a public key. The private key is kept secret by the owner, while the public key is made available to others. Data encrypted using the public key can only be decrypted using the corresponding private key. Conversely, data signed using the private key can be verified using the corresponding public key.

The security of ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), which involves finding the private key that corresponds to a given public key. The ECDLP is considered to be much more difficult than the RSA problem and is considered to be the reason for the security of ECC.

One of the most common uses of ECC is for digital signatures. In digital signatures, the private key is used to sign a message, and the corresponding public key is used to verify the signature. Digital signatures provide a way for a sender to prove that they created a message, and for a recipient to verify that the message has not been altered in transit.

ECC is also commonly used for key agreements, where two parties can agree on a shared secret key without revealing the key to a third party. This is often used in secure communication protocols such as SSL/TLS. It is commonly used for encryption in applications that require high security, such as mobile devices and secure communications.

In terms of levels of security, we can think that ECC provides the same level of security as other public key algorithms with smaller key sizes.Smaller key sizes results in faster encryption and decryption. It can be implemented more efficiently than other public key algorithms, making it a good choice for devices with limited resources, such as smart cards and mobile devices.

In conclusion, the evolution of cryptography has been shaped by the changing needs of individuals and organizations, as well as advances in technology. From simple substitution ciphers used in ancient times to modern public key cryptography and encryption algorithms, cryptography has been used to protect information and facilitate secure communication throughout human history. As technology continues to evolve, cryptography will likely play an even more important role in our daily lives in the future.

Encryption, Decryption, Hashing, and Digital Signatures

We covered loosely, but in broad strokes, cryptography history, and some examples of cryptographic algorithms and uses. However, we will take our time to properly define some of the most important concepts as well as continue our journey surfacing examples.

Encryption is the process of converting data into a format that prevents unauthorized access. If we talk about text, encryption will convert plain text into an unreadable format, known as ciphertext. This is done to protect the confidentiality of the information and ensure that it can only be read by the intended recipient. As previously mentioned, we can use symmetric encryption or asymmetric encryption. Also, as mentioned, symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses two different keys, a public key for encryption and a private key for decryption.

Decryption is the process of converting encrypted data into its original form. Again, using text as an example, decryption is the process of converting ciphertext back into its original form, plain text. The security of the encrypted information depends on the confidentiality of the key. If the key is lost or stolen, the encrypted information can be easily decrypted, so it is important to properly secure the key.

Hashing is a process of converting an input of arbitrary size (called a "message") into a fixed-size output (called a "hash" or "digest"). The hash is a representation of the original message, but it is not possible to determine the original message from the hash alone. It can't be reversed. Hashing is widely used for data integrity verification, indexing data in hash tables, digital signatures, and password checking.

One important property of a good hash function is that it should be computationally infeasible to generate two different messages that produce the same hash (called a "collision"). Another important property is that it should be computationally infeasible to generate the original message from the hash (called "pre-image resistance").

There are several widely used hashing algorithms, including:

- MD5 (Message-Digest Algorithm 5) – 128-bit hash function. Although widely used in the past, it is now considered insecure due to the discovery of collisions.

- SHA-1 (Secure Hash Algorithm 1) – 160-bit hash function. Although still widely used, it is considered insecure due to the discovery of collisions.

- SHA-2 (Secure Hash Algorithm 2) – a family of hash functions with different digest sizes (224, 256, 384, or 512 bits). SHA-2 is considered secure and widely used for data integrity verification.

- SHA-3 (Secure Hash Algorithm 3) – a family of hash functions with different digest sizes (224, 256, 384, or 512 bits). SHA-3 is considered secure and a successor to SHA-2.

- BLAKE2 – a family of hash functions with different digest sizes. BLAKE2 is considered secure and has a faster performance compared to SHA-3 for certain use cases.

Hashing is a one-way function, commonly used to verify the integrity of data. If the message is altered, even if the alteration is minimal, the hash will also change. This allows the recipient to detect any changes to the message. Its use is widespread, since it can be used for data integrity verification, indexing, digital signatures, and password storage. The security of the hash depends on the specific algorithm used, with recent algorithms (SHA-2, SHA-3, BLAKE2) considered secure.

Digital signatures are a form of electronic signature used to verify the authenticity of a message. A digital signature is created by hashing the message and then encrypting the hash with the sender's private key. The recipient can then use the sender's public key to decrypt the signature and compare it to the hash of the original message. If the hashes match, the recipient can be confident that the message came from the sender and has not been altered in transit.

In conclusion, encryption, decryption, hashing, and digital signatures are four fundamental concepts of cryptography that are essential for securing sensitive information and ensuring the integrity of data.

These concepts are used in a variety of applications, from secure communication to password protection, and are critical for ensuring the privacy and security of information in the digital age.

As we know, cryptography plays a crucial role in protecting sensitive information and ensuring the privacy and security of data and communications. In this section, we will discuss three major cryptographic applications: protecting data, communications, and identities.

There are three major things achieved by Cryptography: Protecting Data, Protecting Communications and Protecting Identities.

Protecting Data

Cryptography is commonly used to protect the confidentiality of data stored on computers and servers. Data encryption algorithms such as the one we described like, AES, or even some ones that we did not mention such as Rivest Cipher 4 (RC4) are used to encrypt the data, making it unreadable to unauthorized users. Encrypted data can only be decrypted by someone who has the correct decryption key. In the event that the encrypted data is stolen, it will be unreadable to the attacker and the confidentiality of the data will be maintained.

Protecting Communications

Cryptography is also used to protect the privacy of communication between two parties. The most common example of encrypted communication is Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), which are used to secure the communication between a web browser and a website. When a user visits an SSL/TLS-protected website, the browser and website use a cryptographic protocol to negotiate an encryption key. This encryption key is used to encrypt all subsequent

communication between the browser and the website, providing privacy and security for the user's data.

In order to understand encrypted communications, let's use the example of Bob and Alice. Bob wants to send a message to Alice securely, so he encrypts the message using Alice's public key. The encrypted message can only be decrypted using Alice's private key, ensuring that only Alice can read the message. Alice can then reply to Bob using the same process, encrypting her response with Bob's public key.

Protecting Identities

Cryptography is also used to protect the identities of individuals and organizations in a variety of applications. For example, digital certificates are used to verify the identity of websites and ensure that users are communicating with the correct website. Digital certificates contain the public key of the website, along with information about the website's identity and the identity of the certificate authority that issued the certificate. When a user visits a website, the website's digital certificate is verified by the user's browser, ensuring that the user is communicating with the correct website.

Cryptographic Attacks and Countermeasures

Cryptographic systems are the backbone of secure communication and information protection in the digital world. Despite the many advantages of cryptography, it is not immune to attacks and vulnerabilities. This article will provide an overview of the different types of cryptographic attacks and the countermeasures that can be used to protect against them.

Brute Force Attack

A brute force attack is a straightforward and simple method of trying all possible possibilities of a given security measure. An example is trying all combinations of characters in a password to determine the correct one. The attacker starts with the simplest combination, such as "a", and then moves on to the next, such as "aa", and so on, until the correct password is found. This type of attack can be mitigated by using long and complex passwords, and by using password managers to generate and store strong passwords, as well as rate limiters.

Dictionary Attack

A dictionary attack is similar to a brute force attack, but instead of trying all possible combinations of characters, the attacker uses a dictionary of commonly used passwords to try and guess the correct one. This type of attack can be mitigated in the same way.

Man-in-the-Middle Attack

A man-in-the-middle attack occurs when an attacker intercepts and alters communications between two parties. The attacker intercepts the communication, modifies it, and then passes it on to the intended recipient. This type of attack can be mitigated by using encryption and digital signatures to verify the

authenticity of communications. It can be seen with multiple names and acronyms, such as monster-in-the-middle, machine-in-the-middle, monkey-in-the-middle, meddler-in-the-middle, manipulator-in-the-middle (MITM), person-in-the-middle(PITM) or adversary-in-the-middle (AiTM) attack, depending on the bibliography. These types of attacks can be very sophisticated and even conducted by state sponsored hackers.

Side-Channel Attack

A side-channel attack is an attack that exploits weaknesses in the implementation of a cryptographic system rather than the cryptography itself. Side-channel attacks take advantage of information leaked by the implementation of a cryptographic algorithm, such as the timing of encryption or the power consumption of a device. This type of attack can be mitigated by implementing secure and efficient cryptography algorithms, and by ensuring that the implementation of these algorithms does not leak sensitive information.

Cryptanalysis

Cryptanalysis is the process of analyzing and breaking cryptographic systems. Cryptanalysis attacks can be divided into two categories: theoretical attacks and practical attacks. Theoretical attacks are mathematical attacks that aim to break the cryptography by analyzing the underlying mathematical structure of the algorithm. Practical attacks are attacks that exploit weaknesses in the implementation of cryptography, such as poor key management or weak random number generation. This type of attack can be mitigated by using strong encryption algorithms, implementing secure key management, and using strong random number generation.

Social Engineering Attack

A social engineering attack is an attack that relies on human interaction and deception. The attacker manipulates or convinces individuals to disclose confidential information or to perform actions that compromise the security of a system. This type of attack can be mitigated by raising awareness of the dangers of social engineering, providing training on how to identify and respond to social engineering attacks, and implementing security controls that limit the access of sensitive information.

According to PurpleSec, 98% are involved in social engineering on some level. It could involve pretending to be a trusted contact to encourage an employee to click a malicious link, pretending to be a reliable institution, like a bank, to capture login credentials, or similar activities designed to gain entry into target systems.

Cryptographic attacks pose a significant threat to the security of cryptographic systems, and it is important to understand and be aware of the different types of attacks that exist and the countermeasures that can be taken to prevent or mitigate them. By using strong encryption algorithms, secure key management, and other security controls, organizations can protect their information and ensure the confidentiality, integrity, and availability of their data.

The Future of Cryptography: Emerging Trends and Advances

With the advancements in technology and the growing need for secure communication and data protection, cryptography is becoming increasingly important.

Here are some emerging trends and advances in cryptography:

Quantum Cryptography

Quantum cryptography uses the principles of quantum mechanics to securely transmit information. Unlike traditional encryption methods, quantum cryptography provides guaranteed secure communication as it is based on the laws of physics. The key feature of quantum cryptography is the use of quantum bits, or qubits, instead of classical bits. These qubits can be in multiple states at the same time, making it impossible for an eavesdropper to intercept the information without altering it. This makes quantum cryptography highly secure and is expected to be widely adopted in the future. We will see more about quantum cryptography in the following chapters.

Post-Quantum Cryptography

As quantum computers become more advanced, they are expected to be able to break traditional encryption methods. To prepare for this, a new generation of cryptography algorithms is being developed, known as post-quantum cryptography. These algorithms use mathematical problems that are believed to be resistant to quantum computers, ensuring the security of communication even in the presence of a quantum computer.

Homomorphic Encryption

Homomorphic encryption is a type of encryption that allows computations to be performed on ciphertext, producing an encrypted result which, when decrypted, is equivalent to the result of the computation performed on plaintext. This enables sensitive information to be processed without having to first decrypt it, thus maintaining the privacy of the data.

Zero-Knowledge Proofs

Zero-knowledge proofs are a concept in cryptography that allows one party (the prover) to prove to another party (the verifier) that they know a specific piece of information, without revealing the information itself. In other words, zero-knowledge proofs allow for verifiable statements to be made without revealing any underlying data.

The importance of zero-knowledge proof lies in their ability to protect privacy while still allowing for verifiable statements to be made. They have a wide range of applications in areas such as finance, identity verification, and voting systems. In finance, zero-knowledge proofs can be used to prove the

authenticity of financial transactions without revealing the underlying details, such as account balances or the identities of the parties involved. In identity verification, zero-knowledge proofs can be used to prove that a person is over a certain age without revealing their date of birth. And in voting systems, zero-knowledge proofs can be used to ensure the privacy and integrity of voting results.

Zero-knowledge proofs are based on mathematical algorithms that allow for the creation of proof systems. These proof systems are designed to be both computationally sound (i.e., it is not possible to generate false proofs) and zero-knowledge (i.e., no information is revealed during the proof process). The most well-known zero-knowledge proof system is called ZK-SNARK, which stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge." ZK-SNARKs have been widely adopted in various applications, including cryptocurrency and blockchain technology.

In the context of blockchain technology, zero-knowledge proofs play a crucial role in maintaining the privacy and security of the network. For example, in the cryptocurrency ZCash, zero-knowledge proofs are used to ensure that transactions can be verified without revealing any information about the sender, receiver, or amount involved. This allows for greater privacy and security compared to other cryptocurrencies that store all transaction information on a public ledger.

The future of zero-knowledge proofs is bright, with ongoing research and development aimed at improving their efficiency and scalability. With the increasing importance of privacy and security in the digital world, zero-knowledge proofs are poised to play an increasingly significant role in a variety of industries and applications. Additionally, the development of new zero-knowledge proof systems, such as ZK-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge), holds the potential to further improve the efficiency and scalability of zero-knowledge proofs.

They are a powerful tool for ensuring privacy and security in a wide range of applications and allow for verifiable statements to be made without revealing any underlying information, and their importance is likely to continue to grow as privacy concerns increase in the digital world. With ongoing research and development, the future of zero-knowledge proofs looks bright, and it will be exciting to see where this technology goes in the coming years.

Blockchain Cryptography

Blockchain technology is a decentralized ledger that uses cryptography to secure transactions and protect information. The use of cryptography in blockchain allows for secure and transparent record-keeping, making it ideal for various applications, such as digital currencies and supply chain management.

Blockchain Cryptography refers to the use of cryptographic techniques and algorithms to secure and validate transactions within a blockchain network. The purpose of these cryptographic methods is to ensure the integrity, privacy, and confidentiality of data stored in the blockchain.

Blockchains use public key cryptography to secure and validate transactions. In this method, a pair of public and private keys are used to encrypt and decrypt information. The public key is used for encryption and is shared among the network participants, while the private key is kept secret and is used to decrypt information.

A common cryptographic algorithm used in blockchains is SHA-256, which is a secure hash function that generates a unique digital fingerprint of data. This fingerprint is used to verify the authenticity and integrity of data stored in the blockchain. When a transaction is initiated, the sender uses their private key to encrypt the data, and the recipient uses the sender's public key to decrypt the information.

Another cryptographic technique used in blockchains is called digital signatures. Digital signatures are used to prove that the person who initiates a transaction is indeed the owner of the private key associated with the transaction. Digital signatures use public key cryptography to generate a unique signature for each transaction, which is then verified using the corresponding public key.

Blockchains also use consensus algorithms to validate transactions and add new blocks to the chain. A consensus algorithm is a mechanism that ensures all participants in the network agree on the state of the blockchain. Some common consensus algorithms used in blockchains include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).

Proof of Work (PoW) is a consensus algorithm where participants compete to solve a complex mathematical problem. The first participant to solve the problem is allowed to add a new block to the blockchain, and the solution to the problem is included in the block as proof of work. It is used by the Bitcoin network to validate transactions and secure the network.

Proof of Stake (PoS) is a consensus algorithm where participants are selected to validate transactions and add new blocks to the chain based on the amount of cryptocurrency they hold in the network. In PoS, participants are incentivized to act honestly and validate transactions truthfully, as their stake in the network is at risk if they act maliciously.

Delegated Proof of Stake (DPoS) is a consensus algorithm where participants vote for a limited number of delegates to validate transactions and add new blocks to the chain. DPoS aims to balance security, scalability, and decentralization, and is used by many blockchain networks, including EOS and TRON.

Blockchain cryptography also helps to ensure the privacy of transactions and the confidentiality of data stored in the blockchain. One common method used to achieve privacy in blockchains is called zero-knowledge proofs. Zero-knowledge proofs are cryptographic techniques that allow one party to prove to another party that a statement is true without revealing any information beyond the fact that the statement is true.

For example, a person can use zero-knowledge proof to prove they are over 18 years old without revealing their actual age. This same principle can be applied to blockchains to prove that a transaction is valid without revealing the details of the transaction. Zero-knowledge proofs are used by many privacy-focused blockchain networks, such as Zcash and Monero.

Cryptography is a rapidly evolving field with new trends and advances emerging all the time. From quantum cryptography to homomorphic encryption, these developments are helping to ensure the security of communication and data in our digital world. These technologies are expected to play a critical role in the future of cryptography, ensuring that information remains secure and private even as technology continues to advance.

References

https://purplesec.us/resources/cyber-security-statistics/, February 2023

Aumasson, Jean-Philippe (2021), Crypto Dictionary: 500 Tasty Tidbits for the Curious Cryptographer. No Starch Press, 2021

Aumasson, Jean-Philippe (2017), Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017

Falconer, John (1685). Cryptomenysis Patefacta, or Art of Secret Information Disclosed Without a Key.

Ferguson, Niels, and Schneier, Bruce (2003). Practical Cryptography, Wiley

Goldreich, Oded (2001 and 2004). Foundations of Cryptography. Cambridge University Press.

Katz, Jonathan and Lindell, Yehuda (2007 and 2014). Introduction to Modern Cryptography

A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone (1996) Handbook of Applied Cryptography

https://www.proofpoint.com/us/resources/threat-reports/state-of-phish , February 2023

Kahn, David – The Codebreakers (1967)

CHAPTER 3: The Major Components Of The Zero Trust Framework

In the world of security, not just Cybersecurity, the identification of an individual is not just a requirement these days, it is an absolute must. But the ways about going to conduct this identification process varies from company to company, some require multiple layers of it, and some just require one mechanism in order to fully confirm the identity of the person in question (this will be discussed in detail later on this chapter). Probably the most traditional way of confirming somebody has been the password.

The Password

In fact the password is the dinosaur of identification, having gone back decades. It certainly has proved its over time, but now, given the sophistication of the Cyberattacker, it has literally outlived its usefulness. A primary reason for this is that this is a much sought after prize for the hacker, because after all, once they have a password, all they need to do is somehow guess the username (unless they already have from a previous security breach).

Once this has been accomplished, then their reign of terror can begin. For example, they can drain your bank accounts, and even launch credit card fraud attacks (the author of this chapter has actually been a victim of this). Or this can be sold on the Dark Web for a rather nice profit, along with the other username/password combinations that have been heisted.

Or in a new trend that is happening these days is that the Cyberattacker can actually hire out another firm on the Dark Web and have them launch on attack using the stolen credentials. This has become known as a "Ransomware as a Service" attack. But even though the password has been such a huge target, many people still choose to keep on doing things associated with it as they normally have.

Instead of heeding the warnings of their employers, many people so the following with their passwords:

1) They reuse the same password across multiple platforms;
2) When it is time to reset the password, rather than coming up with something different, they use just slightly different alteration of the original password;
3) They will use a very easy to remember password, some of the following are typical examples that have been used and continue to do so:

   *Password

   *123456

   *123456789

   *12345678

   *1234567

   *Password1

   *12345

   *1234567890

*1234

*Qwerty123

4) They will use other forms to create an easy to remember password, such as a birthdate, name of a relative, or even the name of a previous employer. Now these are obviously a little bit more secure to use that the passwords listed in #3, but they are still very easy to guess, given the use of OSINT (also known as Open-Source Intelligence), and the availability of Social Media profiles.

Because of this, almost 99% of all businesses in Corporate America have now mandated that their employees come up with a much stronger password, one that is much harder to crack and break into. Some of the guidelines for creating these kinds of passwords include the following:

1) Keep the password long. Many Cyber vendors recommend creating a password at least 15 to 16 characters long, and this should interspersed with punctuation, numerical values, and upper- and lower-case letters.

2) Avoid substitutions from previous passwords. The reason for this is because there is a very strong possibility the older one could have been hijacked in a previous security breach, and if it is altered in just a slight way, it could still very well be detected in a later, brute force attack. An example of substitutions include the following:

DOORBELL becoming D00R8377.

3) Be careful of using keyboard shortcuts. If you have any key logger spyware maliciously deployed on your wireless device, ti can track these movements very easily and send them back to the Cyberattacker in a Remote Code Execution (RCE) attack.

4) If you have an existing passphrase created elsewhere, it is recommended that you create a different version of that, using a combination of meaningless words in the process.

5) Another, more superior version of the passphrase is to create a sentence (not too long) as your password. Here is an example:

The Old Duke is my favorite pub in South London

Now becomes.

ThOlDuismyfapuinSoLo

(SOURCE: https://blog.avast.com/strong-password-ideas)

Other examples include the following:

2BorNot2B_ThatIsThe? (To be or not to be, that is the question – from Shakespeare)

22

L8r_L8rNot2day (Later, later, not today – from the kid's rhyme)

4Score&7yrsAgo (Four score and seven years ago – from the Gettysburg Address)

John3:16=4G (Scriptural reference)

14A&A41dumaS (one for all and all for 1 – from The Three Musketeers, by Dumas)

(SOURCE: https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password)

6) Another recommended way to create a very strong password is to use your favorite websites, or the ones that you visit most commonly. Some typical examples of this include the following:

ABT2_uz_AMZ! (About to use Amazon)

ABT2_uz_BoA! (About to use Bank of America)

Pwrd4Acct-$$ (Password for account at the bank)

Pwrd4Acct-Fb (Password for a Facebook account)

(SOURCE: https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password)

7) In some places where a complex password is required, you can even create an emoticon. The caveat here is that you can't use the actual image, you can only create one from the symbols that are available on your keyboard. The following matrix displays this:

!
@
#
$
%
^
&
*
(
)
_
+
{
}
|
"
<
>
-
=
[

]	
;	
\	
'	
,	
.	
/	

Because these newer versions of passwords are far more complex than the easier ones just listed, people still tend to shy away from using these. The answer is quite simple here, as they are too hard to remember. And that is using the Password Manager.

It can be technically defined as follows:

"They store your login information for all the websites you use and help you log into them automatically."

(SOURCE: https://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/)

Essentially, it is a software application package, but comes with the following features:

*It creates long and complex passwords that are hard to crack;

*It stores those passwords;

*It can reset passwords automatically on a preestablished timetable;

*It will keep track of all the websites that you visit, and store that into its memoey;

*It will login into those websites automatically for you;

*It will create passwords for all of the Operating Systems (OS's) that you may be using, including macOS, Windows, Linux, iOS, and Android;

*It will alert you if one your passwords has been hijacked and automatically reset it for you;

*It will even scan the Dark Web for you to make sure that your login credentials do not reside there;

*It can also store your other important documents like your driver's license and insurance card.

To log into a Password Manager, you will need to use another form of authentication, such as a One Type Password (OTP) or something similar to an RSA Token. The former is sent to you as a text on your smartphone. But even despite all of this, unless they are job is dependent upon it, employees still ignore to use this tool. Instead, they would much rather use an easy to remember password, or if they have to remember a long and complex password, they will simply write it down next to their monitor, which will be available in plain sight.

So, what can be done to rectify all of this, if the password is still to be used? This is where the role of Two Factor Authentication, also known as "2FA" comes into play.

24

The Rise of Two Factor Authentication

The last section just reviewed how passwords have been such a crux in our digital society of today. But no matter how much we acknowledge the great, inherent weaknesses that are in them, and even more so, how much we want to get rid of them, the bottom line is that they will still be here for a long time to come. Evern despite the recommendation to further strengthen them, just about a majority of the population here in the United States still like to go back to their old patterns of using passwords, not only putting themselves at greater risk, but the people around them as well.

So the best that can be done here is to build a better mousetrap for authentication, while still using the password. So how does one go about this? Well it comes down to using another authentication tool along with the password. As mentioned earlier, it can range from using a challenge/answer response question to using a smart card. This has now become known as "Two Factor Authentication", or simply known as "2FA.". It can be technically defined as follows:

"Two-factor authentication (2FA) is an identity and access management security method that requires two forms of identification to access resources and data. 2FA gives businesses the ability to monitor and help safeguard their most vulnerable information and networks."

(SOURCE: https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa#:~:text=Two%2Dfactor%20authentication%20(2FA),most%20vulnerable%20information%20and%20networks.)

Simply put, along with the password with another form of authentication. An example of this is illustrated below:
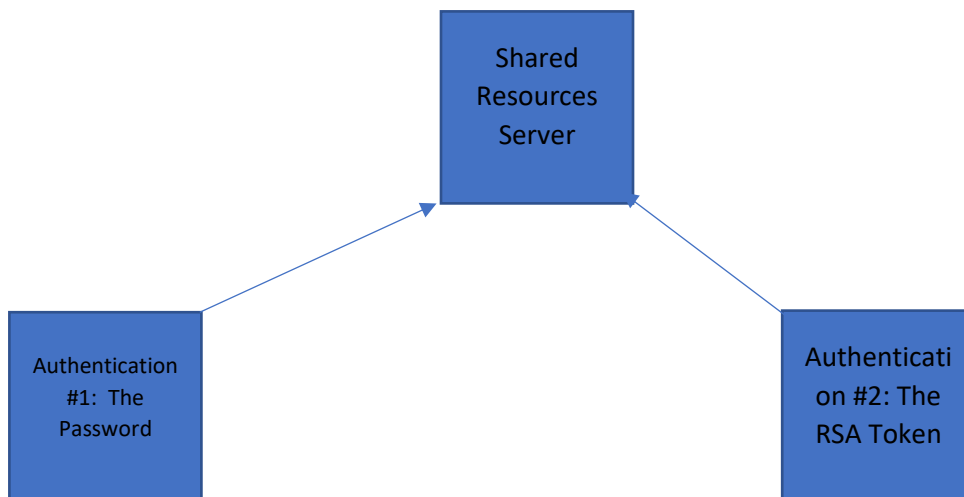
In the above example, the employee is requesting to be authenticated so that he or she can gain access to the server that houses the shared resources that they are needing to complete a certain project. The first level of authentication is entering a password (no matter how easy or complex it actually is), and the second level of authentication is the RSA Token. Once the employee passes through these two hurdles, they can then be granted access to the server.

The primary of using 2FA is obvious: If the Cyber attacker can break through the password, they still have to break through yet another line of defense to get access to the server. And this one will probably prove to be more difficult to crack. There are other types of 2FA tokens, and they include the following:

1) Hardware tokens:

   These are FOBs that produces a brand new, numerical code every few seconds. In fact, the RSA Token works similarly in this manner.

2) Push Notification:

   A One Time Password (also known as an OTP) is sent as a text message to your smartphone. Most of the time it is just a five or six number numerical value that you have to enter in at the website you are trying to get into. Many financial institutions use this technique as a means of confirming your identity.

3) SMS Verification:

   This is when a legitimate link is sent to your smartphone, and you have to click on it in order to gain access. Amazon makes use of this type of verification before you can gain access to your account.

4) Voice authentication:

   This is a much more advanced technique in that Voice Recognition is being used to confirm your identity. It is also another form of a Biometric based modality.

Along with the advantages that 2FA brings, it also has a number of key drawbacks as well, include the following:

1) The user can be locked out:

   Suppose the end user successfully enters in their password, but has difficulty getting passed through the second one. Also assume that this is a legitimate employee as well. This person can be locked after a certain amount unsuccessful attempts (the limit here is usually at three).

2) It can take more time:

   With the technological advancements of today, 2FA should not take more than a few minutes to accomplish. But technology can have certain points of failure, and if the 2FA system is not optimal working mode, it can take even longer to get access. This only adds more to the frustration level of the end user.

3) It can be complex and expensive:

26

For a simple Mom and Pop business, deploying 2FA should be relatively quick and not too expensive. But if you are a Fortune 100 company or so, implementing a 2FA solution can take a much longer time to deploy, and can be much costlier as well, because of the need to hire an outside vendor for the actual deployment.

4) A psychological issue:

The bottom line is that human beings are creatures of habit. Most of the time we like to do things that we are accustomed to doing it, and don't want any change with it. The same is true of 2FA. It can take a long time for employees to get adjusted to this process, and just one bad experience can negate any benefit to be realized. Therefore 2FA needs to be implemented in a phased-in approach, giving your employees time to get used to a different way of authentication.

But probably the biggest disadvantage of 2FA is that once again with the technological advancements that are taking place today, it is now quite probable that the Cyberattacker can break through now both lines of defense. This gives rise to the need of what is known as "Multifactor Authentication", or MFA for short.

Multifactor Authentication

As the name of it suggests, MFA uses more than two authentication mechanisms to confirm the identity of an end user. It must make use of at least three, with even more as needed (in this regard, theoretically, there is no limit that can be placed on this). A technical definition of MFA is as follows:

"It is an authentication method that uses two or more distinct mechanisms to validate a user's identity, rather than relying on just a simple username and password combination. MFA helps prevent unauthorized access to applications and sensitive data, helping organizations defend against identity theft, cyberattacks, and data breaches."

(SOURCE: https://www.cyberark.com/what-is/mfa/)

Although the definition above says two, in the real world, businesses implement at least three or more layers of security. The basic premise of MFA is almost the same as that of 2FA: If one line of defense is broken into, then the second line of defense becomes harder. But as stated in the last section, the Cyberattacker of today is now able to even break through this second line of defense.

So the idea of MFA is that after a few unsuccessful attempts, the Cyberattacker will simply give up in frustration, or if they are still successful, the overall probability of he or she is getting into something valuable (such as the digital assets) becomes significantly lower. So, if a company is hit with a security breach, they may to install even more layers of security, in order to mitigate that particular risk of happening again in the future.

What are some of the benefits of using MFA? They are about the same as 2FA, but are different in some other areas. Here is a sampling:

1) It can provide for limitless security:

Since there is no required number of authentication mechanisms that you have to put into place, theoretically, your security posture could be at almost 100%. But of course in the real world, this is not really feasible.

2) Provides for more lines of defense:

With 2FA, you are only given two layers of security. So if the password were to be known, you are teetering on the edge of being broken into. But with the MFA, since there is more than a layer of security, the statistical odds of this happening are greatly diminished.

3) It affords for more customization:

Although with 2FA you have some degree of flexibility in what you can use for authentication mechanisms. But with MFA, you have a much greater latitude in customizing your solution in order to meet not only the needs of your employees, but your overall security requirements as well.

4) It can work well with SSOs:

These days, many wireless devices already come with an authentication mechanism that is embedded into them. A typical example of this are the newest brands of iOS. They come with both Fingerprint Recognition ("TouchID") and Facial Recognition ("FaceID"). So, you can use or the other to log into your iPhone. This is an example of a Single Sign Solution (SSO). If Apple decided to, it can even implement MFA with this SSO by simply deploying two or more differing authentication mechanisms into the iPhone.

5) Greater chances of compliance:

Today, there is a plethora of data privacy laws, some of the more notable ones are the GDPR, CCPA, PCI-DSS, HIPAA, etc. Because these regulations have their own set of tenets and provisions, it can be quite confusing for a CISO and their IT Security team to know what they need to compliance into. But by having MFA, you are actually increasing the odds that you will actually become compliant, even without you knowing about it.

6) Enterprise mobility is now a reality:

When COVID-19 hit, many companies in Corporate America were left scrambling to find security resolutions to issues that were never encountered before. Probably the biggest example of this is the meshing of the home network with the corporate network, especially from the standpoint of authentication. But with MFA being deployed, this transition has now more or less been smoothened out. Now with the work model being sort of a hybrid based one, proper and 100% authentication is now a must today.
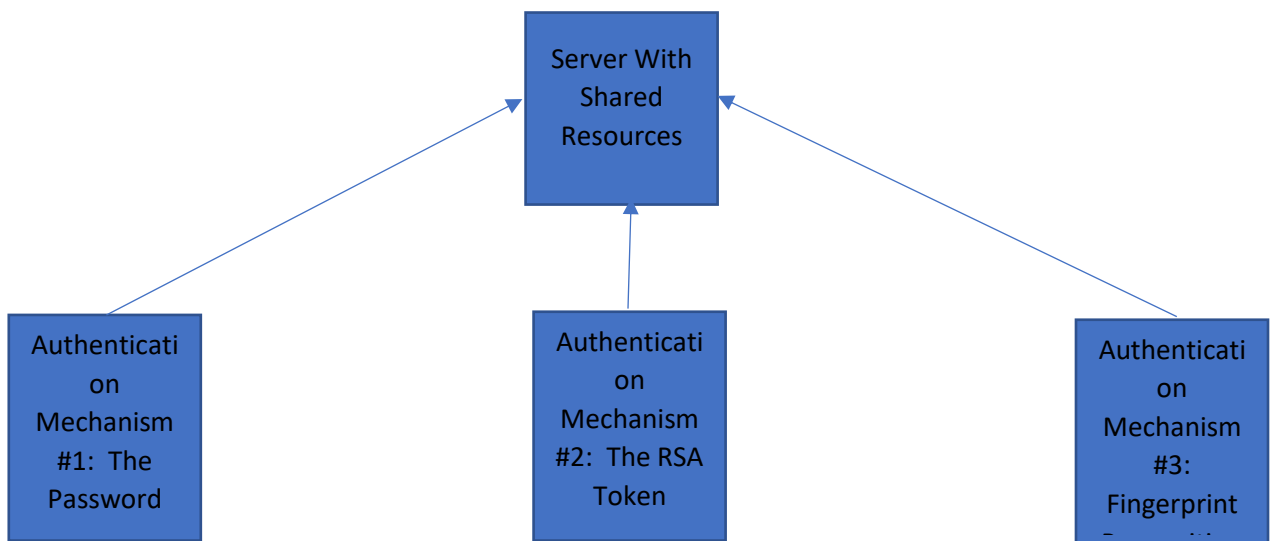
7) More applications for MFA:

By starting out with a larger number of authentication mechanisms, you can now prune out more effectively which ones work and don't with your employees. Here you are taking a trial and use approach, rather simply guessing with a 2FA approach. Although the role of MFA is to protect your shared resources at all costs, you also need to take the time and see which

variation(s) of MFA work best with your employees. After all, they are the ones that will be using it the most, and it is also equally important that you have their buy in as well.

MFA, with its advantages, also comes with its setbacks, and in fact, they are the very same as those for the 2FA, but since there are more authentication mechanisms being used, you can magnify these cons probably to a much larger degree.

A simple MFA is illustrate below:

```
                        ┌──────────────┐
                        │ Server With  │
                        │   Shared     │
                        │  Resources   │
                        └──────────────┘
           ↗                  ↑                  ↖
┌──────────────┐    ┌──────────────┐    ┌──────────────┐
│ Authenticati │    │ Authenticati │    │ Authenticati │
│     on       │    │     on       │    │     on       │
│  Mechanism   │    │  Mechanism   │    │  Mechanism   │
│   #1:  The   │    │  #2:  The RSA│    │     #3:      │
│   Password   │    │    Token     │    │  Fingerprint │
└──────────────┘    └──────────────┘    └──────────────┘
```

In the end, MFA is a far more robust choice to use than 2FA, because it addresses the three needs of authentication which are as follows:

1) <u>Something you know</u>:

   This can be a password, or an answer to a challenge/response question.

2) <u>Something you have</u>:

   This can be an RSA token, a smart card, FOB, etc.

3) <u>Something you are</u>:

   This is typically your Biometrics, whether it is physical or behavioral based.

Technically, you can deploy either the 2FA or MFA into the Zero Trust Framework. But because constant verification is required, MFA has been the top choice so far by many companies who have deployed it. Also, with regard to authentication needs just outlined, it is Biometrics that seems to work the best, although there has been some pushback.

Therefore, the rest of this chapter is devoted to a review of Biometric Technology, with a primary focus on the following types of modalities:

1) <u>Fingerprint Recognition</u>:

   This is where the tip of your fingers are scanned.

2) <u>Iris Recognition</u>:

   This is where the unique features of your Iris are scanned.

3) <u>Facial Recognition</u>:

   This is where the unique features of your face are scanned.

Going forward in this book, whenever we discuss MFA, it will be these three above modalities that will comprise the three authentication mechanisms, as this is what will be used for the Zero Trust Framework, which will be explored in Chapter 5 of this book.

An Introduction To Biometrics

Biometric Technology has actually been around for quite a long time, in fact, going back to the 1960s. This is when the firsthand Geometry Scanners came out, which was used primarily for Physical Access Entry applications. Instead of using a traditional lock and key approach to secure a door, all one had to do was wire this Hand Scanner to an electromagnetic lock strike. After the individual's identity was confirmed by the unique shape and structure of their hand, the lock strike would then unlock, and the door would open up automatically.

The next oldest modality to come out was that of Fingerprint Recognition. Mosty everybody has heard of this, because of its association with law enforcement on a global scale. It was during the height of 9/11 that Biometric Technology picked up a lot of interest. In this case, it was Facial Recognition which received the most attention. However, the technology was still in emerging stages at the time, and it did not live up to all of the hype that the media was giving it.

Once this happened, interest in Biometric Technology started to wane quickly, but then yet picked up momentum again once Cybersecurity started to catch fire. But this time, it did not look like the primary means of defense, just given how expansive and complex Cybersecurity can be. Rather, it is now being looked at as authentication mechanism in a 2FA or MFA role.

But before we move on any further, one may ask at this point, "Why has there always been such an interest in Biometrics?" Well, the truth of the matter is that it is one of the most reliable ways in which to confirm the identity of an individual with near 100% accuracy. The primary reason for this is that it is the unique characteristics of an individual that are being captured. Everybody has unique characteristics; thus this is what makes Biometrics stand out in the world of Identity and Access Management (IAM).

Definition and Unique Features

Now that you have an idea of what Biometrics is about, a technical definition of it can be given as follows:

"A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics."

(SOURCE: https://csrc.nist.gov/glossary/term/biometrics)

As this term has been used repeatedly in this chapter, the key thing here to remember is uniqueness. We all have unique features which separate us from everybody else in the world. The following matrix describes these features that can be used by a Biometric modality:

Biometric	*It's Unique Features*
The Fingerprint	The whorls, valleys, and ridges found on the Fingertip
The Face	The unique distances of the prominent features of the Face
The Iris	The unique orientations of objects that are found in the Iris
The Retina	The unique mapping of blood vessels that are found in the back of the eye, just ahead of the Optic Disc
The Voice	The unique inflections in our Voice when we speak
The Veins	The unique pattern of Veins found underneath the palm
The Keystroke	The unique typing pattern we have when typing on the keyboard
The Signature	This does not refer to the actual signature itself, but the unique mannerisms in which it is signed

So, as you can see from this matrix, there are two general categories of Biometrics:

1) <u>The Physical Biometrics</u>:

   This is where a biological sample is taken from an individual.

2) <u>The Behavioral Biometrics</u>:

   This is where a behavioral sample is taken from the individual.

The Process of Identification

Although Biometrics may sound like a complex piece of technology, it really is not. In an ideal and

optimal situation, a person can be identified in just two or seconds or even less, depending on how recent or old the technology that is being used. Although there is quite a bit that happens behind the scenes during the identification process using Biometric Technology, the following will give a summary of how it actually happens, and it should be enough of a background once we embark on the chapter that reviews the Zero Trust Framework.

1) The Enrollment Process:

In this scenario, a raw image is captured of the physiological (or behavioral) of an individual. A series of images are captured by the camera of the Biometric device, and compiled into one master image. From here, the unique features are extracted, and stored permanently into the database of the Biometric database. This becomes technically the "Enrollment Template". This is illustrated below:

Fingerprint

Biometric Device:

Creation of Master Image

Unique Feature Extraction: Ridges, Whorls and Valleys

Creation of Enrollment Template
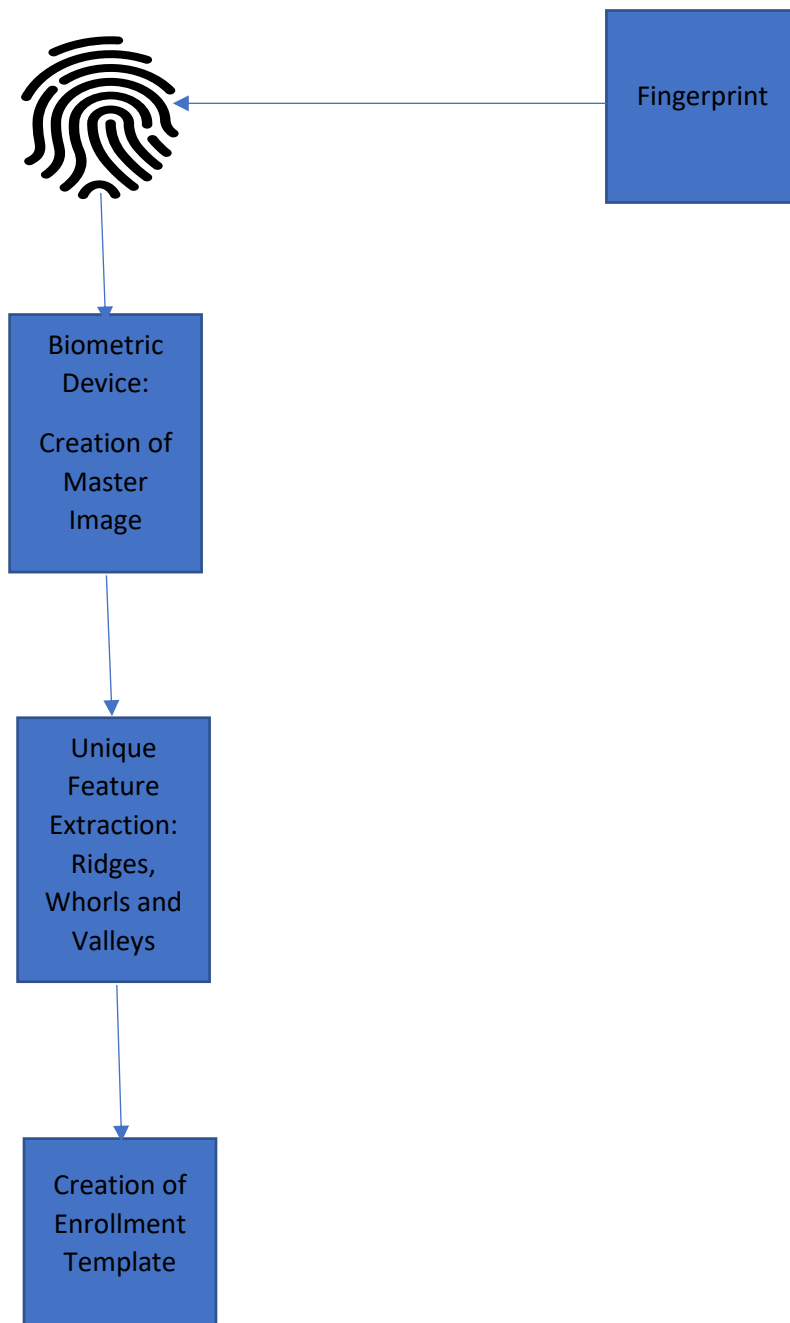
2) The Verification Process:

This is the step where the actual identification happens. But first, the end user must present their fingertip once again to the Biometric device. The same process occurs as in the Enrollment Process. A new brand-new template is now created, and this is called the Verification Template. But this time, the Verification Template is not stored, but instead is compared with the Enrollment Template. If there is a close enough match (or statistical correlation), then the end user is granted authorization to the shared resources that he or she is trying to access. This is illustrated below:
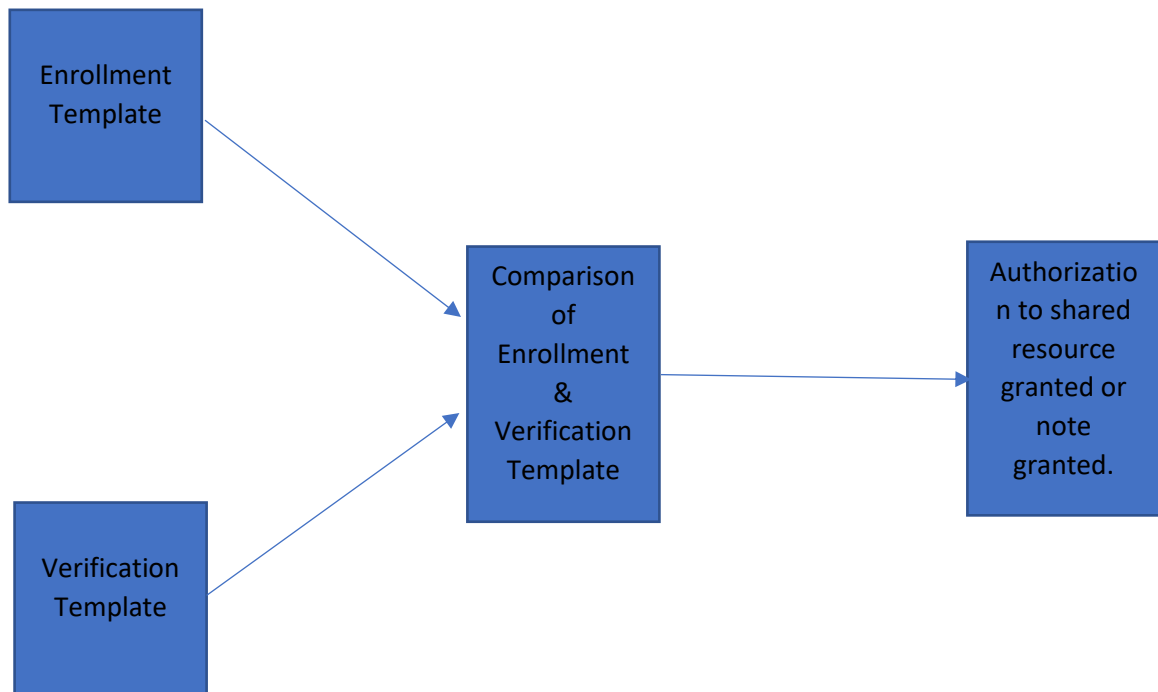
It should be noted that both the Enrollment and Verification templates are not the actual raw images of the fingertip. Rather, it is a mathematical representation of them, and in the case of this example, where Fingerprint Recognition is being used, it is a Binary Mathematical File, consisting of a nothing but a series of zeroes and ones, like this:

IOIO
IOIO

So the question gets asked: "What if a Cyberattacker steals my templates?" Well really, there is nothing to worry about. What can they do about it? Absolutely nothing. It's not like the same as Credit Card theft.

Other Important Concepts

When it comes to the other, relevant concepts of Biometrics, there are plenty of them, but they remain out of the context of this book. But the ones that are relevant to the Zero Trust Framework are related to the performance of the Biometric systems. They specifically deal with the optimization of these system, so that they are working at peak levels in order to keep the Zero Trust Framework infrastructure of a company working on a 24 X 7 X 365 basis.

These concepts are as follows:

- ➢ The False Acceptance Rate
- ➢ The False Rejection Rate
- ➢ The Equal Rate
- ➢ The ability to verify rates.
- ➢ The failure to enroll rate.

1) The False Acceptance Rate:

   This is also known as "FAR", or Type II Errors. This is when an impostor is falsely authenticated by the Biometric system. In the case of the ZTF, this would be the chance that one of the Biometric modalities would actually authenticate and authorize an illegitimate end user into the shared resources server.

2) The False Rejection Rate:

   This is also known as the "FRR", or Type I Errors. This is when a legitimate end user is actually denied access to the shared resources, for whatever reason. For example, there could be a glitch in the Biometric device, or an effective physiological or behavioral set of images was not captured from the end user.

3) The Equal Error Rate:

   This is also known as the "ERR". This is where the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) equal each other out. Actually, this is the optimal point for a Biometric device (or even system) to be at. This is illustrated below:

FRR > FAR

FAR > FRR

% Of Error

The Equal Error Rate (ERR)

Threshold Setting
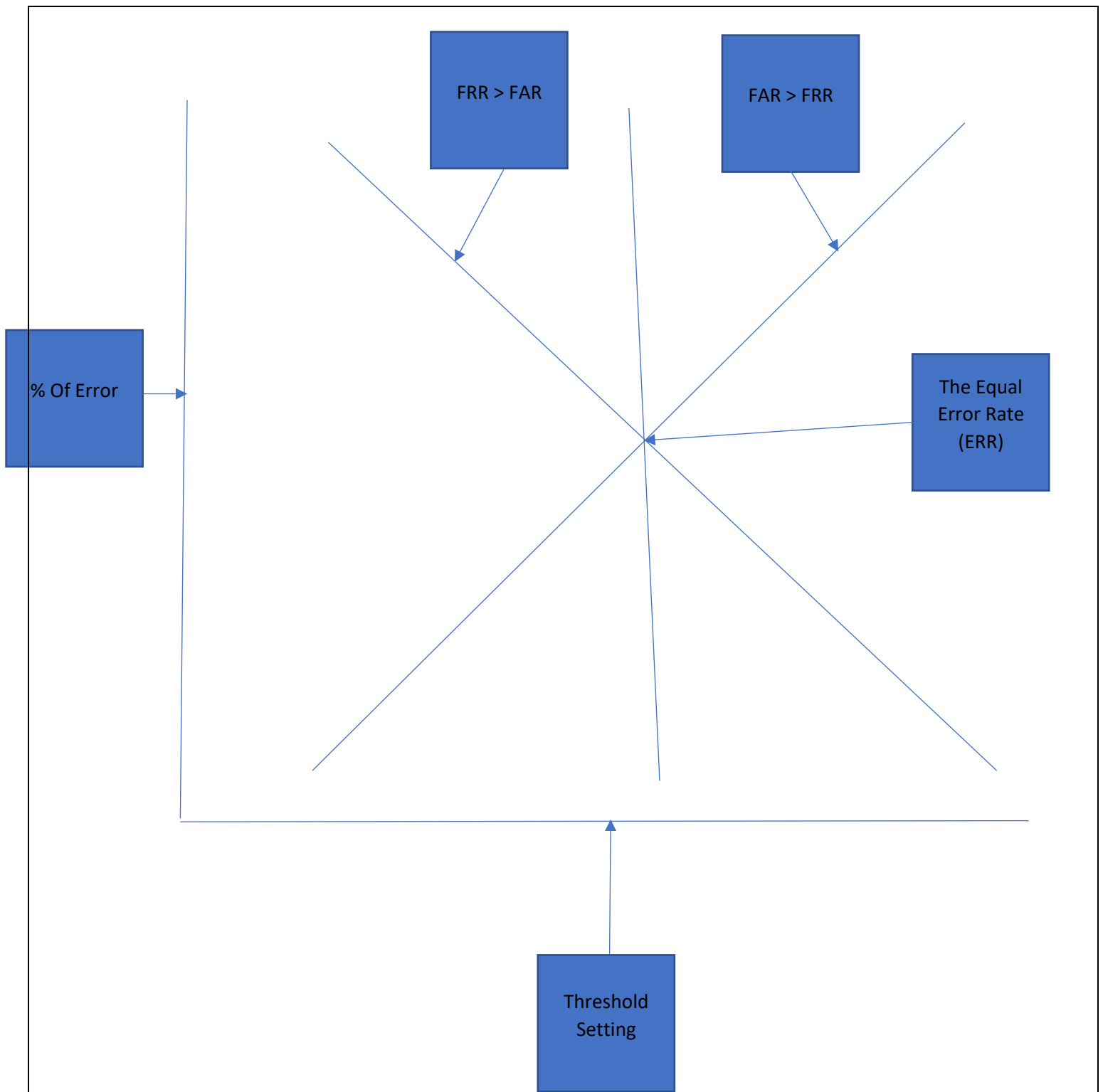
4) The Ability To Verify Rate:

This is also known as the "AVR", and this metric reflects the total percentage of the end user base that that can be legitimately enrolled into a Biometric modality. With the Zero Trust Framework, this is the total number of employees that can be legitimately enrolled in all of the three Biometric modalities, and even more if necessary.

Mathematically, this can be represented as follows:

$$AVR = [(1 - FER) * (1 - FRR)$$

5) <u>The Failure to Enroll Rate</u>:

This is also known as the "FER". This metric reflects the overall percentage of the population that cannot be enrolled into a Biometric system. With respect to the Zero Trust Framework, this reflects the total number of the employee population that cannot be enrolled into a Biometric system, for whatever reason, whether it is a flaw in the technology itself, or the end user has some physical ailment that is prohibiting he or she from being enrolled into the Biometric system.

Ultimately, it is up to the security requirements of the business as to where the ideal threshold should be at. Although the Equal Error Rate (ERR) is the ideal place to be at, this is only theoretical. The ideal point would be somewhere where the FRR > FAR. But keep in mind that in the Zero Trust Framework, if the Cyber attacker were to gain access to one Biometric system, they still have two more to through, and the chances of getting through those are almost nil.

The Biometric Sensor

In the Zero Trust Framework infrastructure, when it comes to the Biometric devices themselves, a camera in the device itself is used to capture the raw images of the fingerprint, iris, and face. But for the longest time, Fingerprint Recognition has made use of a direct contact sensor. There are many vendors out there who still use this, but now the trend is, after the COVID-19 pandemic, to use non contactless image capture technology, like in the case of Facial Recognition and Iris Recognition.

Fingerprint Recognition devices have typically used what are known as "Optical Sensors". In this kind of set up, the end user places their fingertip on top of a platen. It is usually made from a glass composite and just underneath the platen, a Light Emitting Diode (LED) a light is flashed towards the optical sensor, and is magnified by using a Charged Couple Device (CCD). It is essentially a camera that transform any light pattern into a series of electrons.

Now, as the fingertip is placed onto the platen the light (as just described) captures the ridges of the fingerprint back into the CCD. The ridges (from where the bulk of the unique features are captured from) appear as solid, dark lines.

Another alternative to the Optical Sensor is what is known as the Solid-State sensor. But rather than using a CCD, they use electrode arrays to capture the image of the ridges of the fingerprint. To get the raw images of the fingertip, a capacitance level is formed between the fingertip and the electrode. There are two types of Solid-State sensors:

1) Many electrodes in which the entire image of the fingertip can be captured.
2) Fewer electrodes used a sweeping mechanism, to capture the full image of the fingertip, by going left to right or right to left.

With regards to the non-contactless technology (as mentioned before) there are three kinds of sensors:

1) <u>Reflection based</u>:

A light is shone onto the fingertip from different angles, using just one kind of camera.

2) <u>Transmission based</u>:

A specialized red light is shined through the fingertip. Then this light is aimed towards the sides of the fingertip.

3) <u>Three dimensional</u>:

Two different types of 3D scanning can be used:

*Parametric Modeling: The images of the fingerprint are projected onto a cylindrical model and then from there, then onto a 2D print.

*Non-Parametric Modeling: Various mathematical algorithms are used to model the ridges of the fingertip, and are thus powerful enough to take into account any irregularities of the fingertip.

So as you can see, sensor technology, albeit a small component in the grand scheme of things, still plays a critical role in keeping the Zero Trust Framework infrastructure humming along. Any hiccups here can still have a huge impact.

Now that we have gone over some of the major principles of Biometrics in general, the rest of the chapter is devoted to reviewing in more detail the following Biometric modalities which will be used in the Zero Trust Framework:

➢ Fingerprint Recognition
➢ Iris Recognition
➢ Facial Recognition

A Review Of Fingerprint Recognition

The raw images 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: This includes the shapes and the images of the ridges, and their associated pores.

Along with the ridges (as stated in this chapter) are a prime source for unique feature extraction. But there are other features as well, and they include the following:

1) Arches:

    These are the ridges which just flow in one direction, without doubling back, or going backwards. These only comprise about 5% of the features of the fingerprint;

2) Loops:

    In this feature, the ridges go backwards, and go from either the left to the right or the right to the left. There are two distinct types of loops: a) Radial loops which go downward; and b) the ulnar loop which goes upwards on the fingerprint. These make up 65% of the features within the fingerprint;

3) Whorls:

    The ridges in the fingerprint make a circle around a core, and these comprise 30% of the features in the fingerprint.

In addition to the above features which are collected by a fingerprint recognition system, the actual number of ridges, and the way that these ridges are positioned (specifically their orientation) can also prove to be a very distinctive feature as well, and can help to contribute to the verification and/or identification of an individual.

<u>The Process of Fingerprint Recognition</u>

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

1) <u>Raw Data Acquisition</u>:

    The actual, raw images of the fingerprint are acquired through the sensor technology which is being utilized. This means that the raw images which are collected are eventually 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) Unique feature extraction:

With the raw images which have now been 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) Authentication & Authorization:

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 wither physical or logical access to which they are seeking.

<p align="center">Fingerprint Recognition Quality Control Checks</p>

The need to collect high quality, raw images the first time is of paramount importance for the Zero Trust Framework. The following are the quality control checks for fingerprint recognition:

1) Resolution:

This refers to the total number of dots per inch (DPI), or also known as the total pixels per inch (PPI). Most fingerprint algorithms require a DPI or PPI resolution of at least 250 to 300 DPI.

2) Area:

This is the actual size of the scanned and captured fingerprint image. You need to have a minimum scanned fingerprint area of at least one square inch. Anything less than that will not produce a good quality, raw image.

3) Frames Per Second:

This is the total number of raw images the fingerprint recognition device sends to the processing unit. Of course, the higher number of frames per second means a much greater tolerance for any unwanted movements of the fingerprint on the platen.

4) The Number of Fingerprint Pixels:

This refers to the total number of pixels in the scanned image.

5) The Dynamic Range:

This refers to the possible ranges which are available for the encoding of each pixel value, the at least eight bits is optimal.

6) Geometric Accuracy:

These are the geometric differences between the enrollment and the verification templates, and this is calculated via the deviations from the X and Y axes on the fingerprint template.

7) The Image Quality:

This is the variable which refers to the identifying, unique features in the fingerprint, such as the ridgeline patterns and the various minutiae which are extracted.

The second modality in line for the MFA component of the Zero Trust Framework is that of Facial Recognition, and is reviewed in the next section.

A Review Of Facial Recognition

Facial recognition technology relies upon the physical features of the face (see Figure #5) 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.

The unique features that are captured 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.

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 (with the technology that is available today, facial recognition can literally be implanted in a CCTV).

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 much more 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.

<u>The Techniques Of Facial Recognition – Unique Feature Extraction</u>

There are two techniques that are involved with Facial Recognition, which are as follows:

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, and no 3-Dimensional models are every utilized. 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 after that point onwards, the facial variations can be captured and computer. The specific methodology here includes Elastic Bunch Graph Mapping. All of these techniques will now be discussed in greater detail.

With Principal Component Analysis (this is linear based, also known as PCA), this technique dates all the way back to 1988, when it was first used for facial recognition. This technique primarily uses what is known as "Eigenfaces". Simply put, Eigenfaces are 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 placed over the raw images, and are superimposed over one another. 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 if you will, 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 Principal Component Analysis), 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.

With Linear Discriminant Analysis (this is linear based, also known as LDA), the is to project 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.

41

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, but still, a full-face image is required.

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

With the Elastic Bunch Graph Matching (this is model based, also known as EBGM) technique, this looks at the nonlinear mathematical relationships of the face, which includes such factors as 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, and an example of this can be seen in. 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 at all require a full facial image, the main drawback with this technique is that the landmarks of the facial map must be marked extremely accurately, with great precision.

The next section now looks at the third Biometric modality to be used in the Zero Trust Framework, this is Iris Recognition. This is what will give the MFA its very powerful features because Iris Recognition is deemed to be the most powerful modality of all, given its deep and unique features.

Iris Recognition

Iris recognition has developed so quickly that now images of the iris can be captured at much greater distances, as well as when people are in movement. Previously, an end user had to stand directly in front of the iris recognition camera, at a very close proximity. And now, even the unique pattern of the blood vessels can also be scanned, and this will be examined after the section on retinal recognition.

<p align="center">The Physiological Structure of The Iris</p>

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, and in remote cases, even a hazel color can occur. And in even in the most extreme cases, a combination of these colors can be seen in the iris. 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 at about this happens at about the third month 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 stroma is in turn connected to a grouping of muscles known as the sphincter muscles.

It is this muscle which is responsible for the contraction of the pupil, and another group of muscles known as the dilator muscles govern the expansion of the pupil. When you look at your iris in the mirror, you will notice a radiating pattern. This pattern is known as 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, 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). Other unique features can also be seen in the collaretta region. 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. In fact, even scientific studies have shown that even identical twins have different iris structures.

Iris Recognition: How It Works

The idea of using the iris to confirm the identity of an individual dates back to 1936, when an ophthalmologist by 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. Special 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 binary mathematical file, which is not greater than 500 bytes. Because of this very small template size, verification of an individual can occur in just less than one second.

From within the 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 percentage do the zeroes and the ones in the iris-based enrollment and verification templates match up and do not match up against one another? This answer is found by using a technique known as "Hamming Distances", which is even used in iris recognition algorithms of today.

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.

Conclusions

Overall, this chapter has examined some of the major components that make up the Zero Trust Framework:

1) Two Factor Authentication (2FA);
2) Multifactor Authentication (MFA);
3) Biometric Technology.

Going forward into the rest of this book, only MFA will be considered for the Zero Trust Framework, which will be examined in greater detail in the Chapter of this book. In the author's view, the use of 2FA will soon be outnumbered, as the Cyberattacker is now well prepared to break into two lines of defense, and perhaps even more. This is why MFA is so important.

With the extra layers of defense that it presents, it lessens the statistical odds that a Cyberattacker will break through all of the lines of authentication. In theory, this is possible with the other types of authentication mechanisms, but so far this has not proven to be the case with Biometric Technology. The primary reason for this is that it is almost close to impossible, if not difficult, to replicate somebody's fingerprint, and especially the iris.

There are still some doubts about the face, but the reason it was included is that it provides for a still very valuable line of defense, and that it is as non-contactless as well, given the society that we live in today. Also, the other Biometric Technologies (as they were examined earlier in this chapter), still have some ways to go in terms of commercial adoption, thus they would not be a good choice for a Zero Trust Framework.

Also going forward into the rest of the book, the order of arrangement for the Biometric modalities in terms of authentication will be as follows: Fingerprint Recognition, Iris Recognition. This is illustrated in the diagram below:
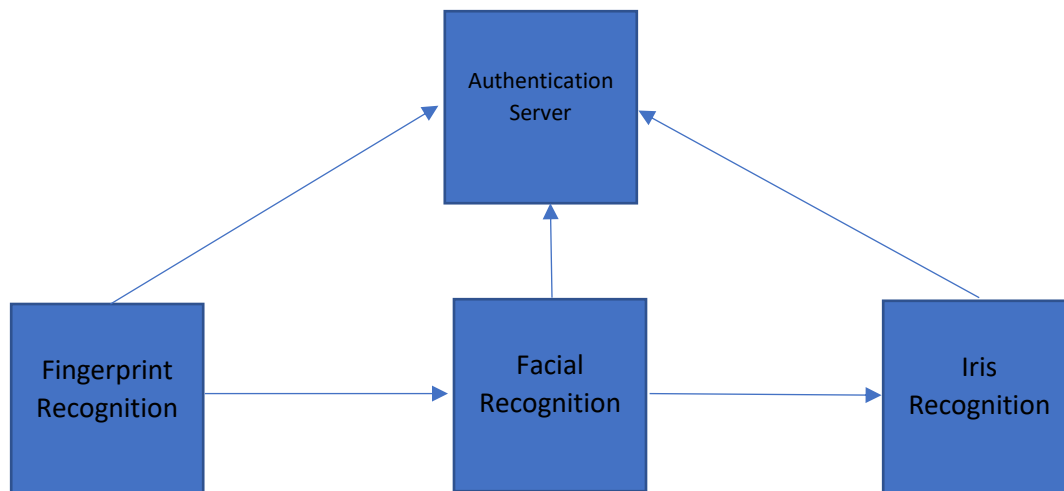
The next chapter of this book will do a greater examination of what is known as "BioCryptography". This is when the principles of Cryptography are used to further protect the Biometric Templates.

CHAPTER 4: The Implementation Of BioCryptography

Introduction

Our last chapter reviewed some of the fundamental components that belong to the Zero Trust Framework. It reviewed in detail the concepts of 2FA, MFA, and the Biometric Technologies that are to be used in any kind of Zero Trust deployment. In the end, it was concluded that MFA and the use of Biometrics as the authentication mechanisms would prove to be of most value and importance to a Zero Trust Framework (ZTF).

In the examples that we provided in the last chapter they all shared one common denominator: It was assumed that there was only one user accessing one shared resource. In terms of mathematics, this can be represented as a one to one, or 1:1 relationship. But in the real world, ZTF deployments will not be this direct. Rather, they will be more complex in nature, and utilize an approach in which there will be many employees accessing many different types and kinds of shared resources, possibly even across different servers that are physically located apart from one another.

Thus, in this case, you want a ZTF which will take the form of what is known as an "Asymmetric Key Cryptography" approach. This is where both public and private keys are used to further protect the Biometric Templates as they are in transit from the point of authentication to the point authorization. As it was mentioned in the previous chapter, Biometric Templates are quite strong in nature.

They are nothing but mathematical based representations of our unique physiological and/or behavioral traits. In the end, if the Cyberattacker were to break through a database and hijack them, there is hardly anything much that they can do with them. As pointed out before, it is not the like the same thing as credit card theft, where a hacker can literally run "amuck" with it, and make all kinds of fraudulent purchases with it.

But the fact that a Cyberattacker can even entertain the thoughts of heisting these Biometric Templates which are so crucial to a ZTF means that there is an inherent weakness in the framework that needs to be remediated, and this can only be done by using the principles of Cryptography. Thus, it is the Asymmetric Key approach which can provide the best protection for this Biometric Templates. This methodology is also referred to as the "Public Key Infrastructure", or "PKI" for short, and this referencing will be used throughout the remainder of this book.

In this chapter, we will lay down the foundations for the PKI, which will be the model used to support our Zero Trust Framework model in Chapter 5. After we introduce the concepts of what it takes to protect these Biometric Templates, the next point of issue that will be dealt with is how to ensure the integrity of these Biometric Templates remain intact from the point of authorization to the point of authentication, as they will be reused over constantly in order to grant access to the shared resources the end user is trying to gain access to.

The ultimate goal here is once the employee has been enrolled into all three Biometric modalities, they will never have to do it again, unless of course something catastrophic happens, such as a natural disaster or security breach occurring. Therefore, it is of paramount importance to make sure that the Biometric Templates remain the same all of the time, without any alterations being made to them.

There is one solution for this, and that is making use of Hashing Algorithms, which will be covered at the end of this chapter.

Also, this will give rise to the need for Privileged Access Management, or PAM, to make sure that all of the access accounts of the employees remain secure and are assigned properly, since the intention is to avoid having to go through the authentication process repeatedly (and only once). This is a concept that will be further explored in Chapter 5 of this book.

An Overview Into The Public Key Infrastructure (PKI)

A PKI can be a very large undertaking, or even just a smaller one, depending upon the size and the requirements of the company in question. But generally speaking, setting up a PKI takes more time than it does using a Symmetric Key Cryptography approach. This kind of approach would be ideal to use in the examples that we have provided so far in this book, as we have assumed thus far that it has been just one employee trying to access one shared resource.

But you do not see this approach being used in the real world, because of the many security risks that it can pose. Therefore, the use of the PKI remains to be the viable choice. In the rest of this chapter, we will introduce the important concepts of the PKI. We will then move onto the topic of BioCryptography, which is the science of using Cryptography to protect Biometric Templates. Finally, we will then delve into the topic of Hashing Algorithms.

What It Is All About

In the world of PKI, there are two primary keys that are used, and they are called the public and the private key, and are also used to encrypt and decrypt the plaintext which is sent between the sending and the receiving parties as they communicate with another. In the most simplistic terms, a PKI can be likened to that of a safety box at a local bank. In this example, normally, there are two set of keys which are used.

One key is the is the one which the back gives to you. This can be referred to as the public key because it is used over and over again by past renters of this particular safety deposit box, and for other, future renters as well. The second key is the private key which the bank keeps in their possession at all times, and only the bank personnel know where it is kept.

A PKI is just like this example, but of course, it is much more complex than this in practice. To start off with, typically, it is the receiving party which is primarily responsible for generating both the public and the private key. In this situation, let us refer to the public key as "pk", and the private key as "sk".

So, to represent both of these keys together, it would be mathematically represented as (pk,sk). It is then the sending party which uses the public key (pk) to encrypt the message they wish to send to the receiving party, which then uses the private key (sk) which they have privately and personally formulated to decrypt the encrypted ciphertext from the sending party.

One of the primary goals of a PKI is to avoid the need for both the sending and the receiving parties from having to meet literally face to face in order to decide on how to protect (or encrypt) their communications with another. So, at this point, the question that arises is, how does the sending party

know about the public key (pk) generated by the receiving party so that the two can communicate with each other?

The Public Key & The Private Key

There are two distinct ways in which this can be accomplished:

1) The receiving party can deliberately and purposefully notify the sending party of the public key (pk) in a public channel, so that communications can be initiated;

2) The sending party and the receiving party do not know anything about each other in advance. In this case, the receiving party makes their public key known on a global basis, so that whoever wishes to communicate with the receiving party can do so, as a result.

Now, this brings up a very important point: The public key is literally "public", meaning that anybody can use it. So, how does a PKI remain secure? It remains solely in the privacy of the private key (sk) which is being utilized. In these cases, it is then up to the receiving party now to share the private key (sk) with any other party, no matter how much they are trusted.

If the privacy of the secret key (sk) is compromised in any way, then the security scheme of a PKI is totally compromised. In order to help ensure that the private keys remain private, the PKI uses the power of prime numbers (also known as the "RSA algorithm"). The basic idea here is to create a very large prime number as a product of multiplying two very large prime numbers together.

Mathematically put, the basic premise is that it will take a hacker a very long time to figure out the two prime number multiples of a very large product which is several hundred integers long, and thus, give up in frustration. Even if a hacker were to spend the time to figure out one of these prime numbers, the hacker still has to figure out the other prime number, and the chances that they will figure this out is almost nil.

As a result, only one portion of the (pk, sk) is figured out, and the PKI still remains intact and secure. In other words, the hacker cannot reverse engineer one key to get to the other key to break the ciphertext. It should also be noted than in the PKI, the same public key can be used by multiple, different sending parties to communicate with the single receiving party, thus forming a one to many, or 1:N mathematical relationship.

This is illustrated in the diagram below:
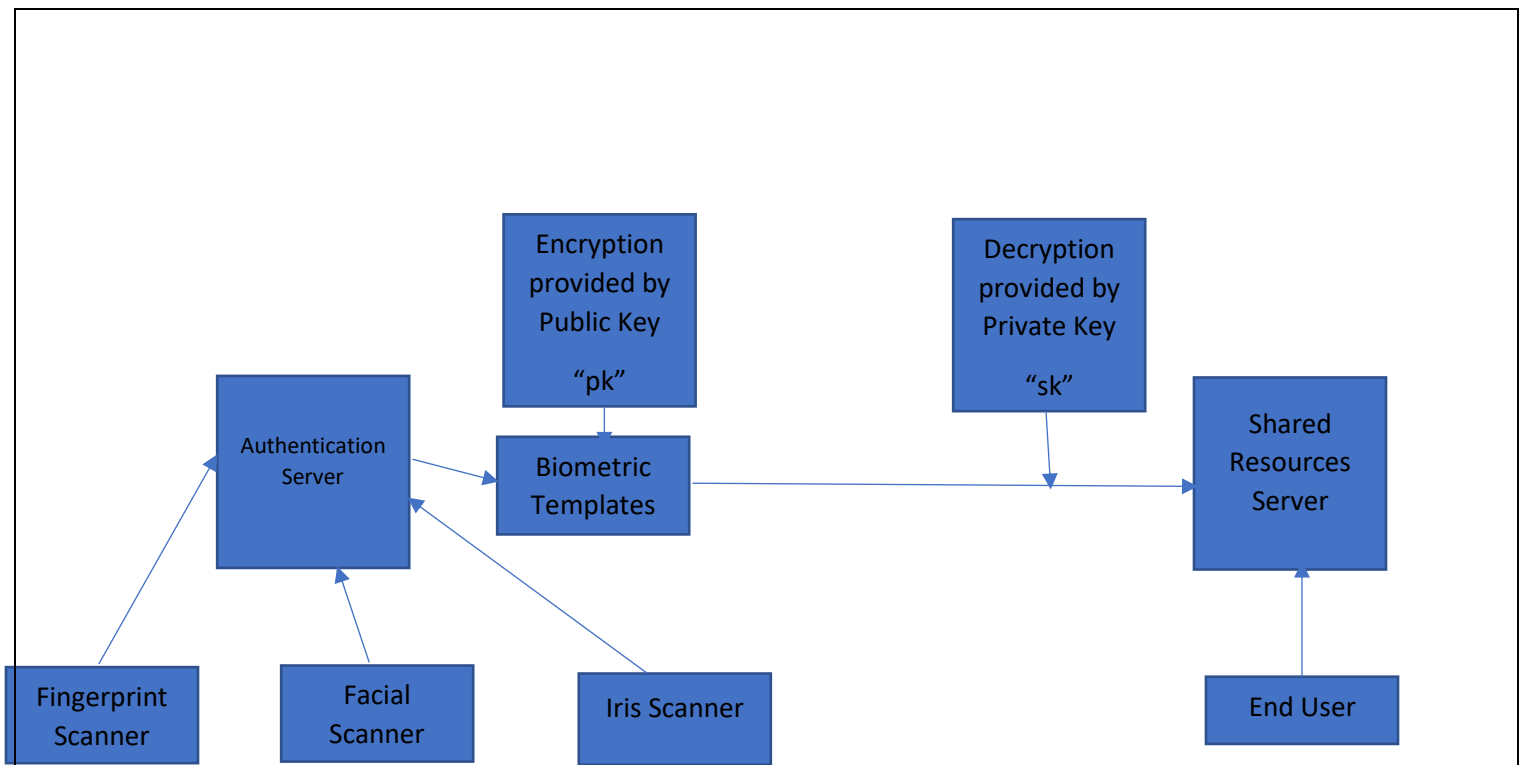
<u>The Mathematical Algorithms of The PKI</u>

There are number of key mathematical algorithms which serve as the crux for PKI, They are as follows:

1) <u>The RSA Algorithm</u>:

   In terms of the RSA Algorithm, this is probably the most famous and widely used PKI cryptography algorithm. In fact, this very algorithm will serve as the foundation for BioCryptography later in this chapter. The RSA Algorithm originates from the RSA Data Security Corporation, and is named after the inventors who created it, which are: Ron Rivest, Adi Shamir, and Leonard Adelman.

   As it was just reviewed previously, the RSA Algorithm uses the power of prime numbers to create both the public key and the private key. But, using such large keys to encrypt such large amounts of data is totally infeasible, from the standpoint of the processing power and central server resources. Instead ironically, the encryption is done symmetric algorithms (such as the ones reviewed previously), then the private key gets further encrypted by the receiving party's public key.

   Once the receiving party obtains their ciphertext from the sending party, then the private key generated by the symmetric cryptography algorithm is decrypted, then the public key which was generated by asymmetric cryptography can then be subsequently used to decrypt the rest of the ciphertext.

2) <u>The Diffie-Hellman Algorithm</u>:

In terms of the Diffie Hellman asymmetric algorithm, it is named after its inventors as well, whom are Whit Diffie and Martin Hellman. It is also known as the DH algorithm for short as well. But interestingly enough, this algorithm is not used for the encryption of the ciphertext, rather the main concern of it is to address the problem of finding a solution to the issue of sending a key over a secure channel.

Here is a summary of how it works on a very simple level:

*The receiving party as usual has the public key and the private key that they have generated, but this time, they both are created by the DH Algorithm;

*The sending party receives the public generated by the receiving party and uses this DH Algorithm to generate another set of public keys and private keys, but on a temporary basis;

*The sending party now takes this newly created temporary private key and the public key sent by the receiving party to generate a random, secret number-this becomes known as the "session key";

*The sending party uses this newly established session key to encrypt the ciphertext message, and sends this forward to the receiving party, with the public key that they have temporarily generated;

*When the receiving party finally receives the ciphertext from the sending party, the session key can now be derived mathematically;

*Once the above step has been completed, the receiving party can now decrypt the rest of the ciphertext.

3) The Elliptical Wave Theory Algorithm:

Finally, with Elliptical Wave Theory, it is a much newer type of PKI mathematical algorithm. It can be used to encrypt very large amounts of data, and its main advantage is that it is very quick, and does not require a lot of server overhead or processing time. As its name implies, Elliptical Wave Theory first starts with a parabolic curve drawn on a normal x,y coordinate Cartesian plane.

After the first series of X and Y coordinates are plotted, various lines are then drawn through the image of the curve, and this process continues until many more curves are created and their corresponding, intersecting lines are also created.

Once this process has been completed, the plotted X and Y coordinates of each of the intersected lines and parabolic curves are then extracted. Once this extraction has been completed, then all of the hundreds and hundreds of X and Y coordinates are then added together in order to create the public and the private key. But the trick to decrypting a ciphertext message encrypted by Elliptical Wave Theory is that the receiving party has to know

the shape of the original elliptical curve, and all of the X and Y coordinates of the lines where they intersect with the various curves, and the actual starting point at which the addition of the X and Y coordinates first started.

<p align="center">The Components Of The PKI</p>

It should be noted at this point that the Public Keys and the Private Keys in a PKI are also referred to as "Digital Certificates". Thus, going forward in this book, that is how they will be referred to. The components of a PKI, and as it relates to the Zero Trust Framework, are as follows:

1) The Certificate Authority, also known as the CA:

   This is the outside third party who issues the digital certificates.

2) The Digital Certificate:

   As mentioned, this consists of both the private key and the public key, which are issued by the CA. This is also the entity that the end user would go to in case he or she needed to have a digital certificate verified. These digital certificates are typically kept are the points of authentication and authorization, respectively.

3) The LDAP or X.500 Directories:

   These are the databases which collect and distribute digital certificates from the CA.

4) The Registration Authority, also known as the RA:

   If the place of business or organization has a large ZTF (such as a multinational corporation), this entity then usually handles and processes the requests for the required digital certificates, and then transmits those requests to the CA to process and create the required digital certificates.

The CA can be viewed as the main governing body, or even the king of the PKI of the ZTF. In order to start using the Public Key Infrastructure to communicate with others, it is the Certificate Authority which issues the digital certificates, which once again, consists of both the public and private keys.

<p align="center">The Digital Certificates</p>

Each digital certificate which is generated by the Certificate Authority consists of the following technical specifications:

1) The Digital Certificate Version Number:

   Typically, it is either version number 1, 2, or 3.

2) The Serial Number:

This is the unique ID number which separates and distinguishes a particular Digital Certificate from all of the others (this can be likened to each Digital Certificate having its own Social Security Number).

3) The Signature Algorithm Identifier:

This contains the information and data about the mathematical algorithm used by the Certificate Authority to issue the particular Digital Certificate.

4) The Issuer Name:

This is the actual name of the Certificate Authority which is issuing the Digital Certificate to the place of business or organization.

5) The Validity Period:

This contains both the activation and deactivation dates of the Digital Certificates, in other words, this is the lifetime of the Digital Certificate as determined by the Certificate Authority.

6) The Public Key:

This was created by the Certificate Authority.

7) The Subject Distinguished Name:

This is the name which specifies the Digital Certificate owner;

8) The Subject Alternate Name Email:

This specifies the Digital Certificate's owner Email address (this is where the actual Digital Certificates go to);

9) The Subject Name URL:

This is the Web Address of the place of business or organization to whom the Digital Certificates are issued to.

How Public Key Infrastructure Works

Below is a description of how the PKI would work for a ZTF:

1) The request for the Digital Certificate is sent to the appropriate Certificate Authority;

2) After this request has been processed, the Digital Certificate is issued to the person who is requesting it;

53

3) The Digital Certificate then gets signed by confirming the actual identity of the person who is requesting that particular Digital Certificate;

4) The Digital Certificate can now be used to encrypt the plaintext into the ciphertext which is sent from the sending party to the receiving party.

The Registration Authority, also known as the RA, as eluded before. The RA is merely a subset of the CA, or rather, it is not intended to replace or takeover the role of the CA, instead, it is designed to help if it becomes overwhelmed with digital certificate request traffic.

However, the RA by itself does not grant any type or kind of digital certificates, nor does it confirm the identity of the person who is requesting the digital certificate. Rather, its role is to help process the requests until the processing queue at the CA becomes much more manageable.

The RA sends all of the digital certificate requests in one big batch, rather than one at a time. This process is known as "chaining certificates". The RA is typically found in very large, multinational corporations, where each office location would have its own RA, and the CA would preside at the main, corporate headquarters.

Finally, all digital certificate requests are processed by the RA and are also associated with a chain of custody trail, for security auditing purposes. The RA can be viewed as a support vehicle for the CA, in which a mathematical, hierarchal relationship exists.

<div align="center">Public Key Infrastructure Policies & Rules</div>

It should be noted at this point that in order for either the Certificate Authority or the Registration Authority to function properly in a Zero Trust Framework, it is important to have a distinct set of rules policies in place. These surround the use of the issuance, storage, and the revocation of the expired digital certificate. While it is out of the scope of this book to get into the exact details of all these rules and policies, the following is just a sampling of some of the topics which need to be addressed:

1) Where and how the records and the audit logs of the Certificate Authority are to be kept, stored, and archived;

2) The administrative roles for the Certificate Authority;

3) Where and how the public keys and the private keys are to be kept, stored, and also backed up;

4) What is the length of time for which the public keys and the private keys will be stored;

5) If public or private key recovery will be allowed by the Certificate Authority;

6) The length of the time of the validity period for both the public keys and private keys;

7) What will be the technique in which the Certificate Authority can delegate the responsibilities to the Registration Authority;

8) Will the digital certificates to be issued by the Certificate Authority be used for applications and resources;

9) If the digital certificates to be issued by the Certificate Authority be used for the sole purposes of just encryption of the ciphertext;

10) If there are any types or kinds of applications which should be refused to have digital certificates;

11) When a digital certificate is initially authorized by the Certificate Authority, if there is a finite period of time when the digital certificate will be subject to revocation.

As one can see, based upon the establishment of the many rules and policies which need to be set into place, the actual deployment and establishment of a Public Key Infrastructure in a ZTF can become quite complex, depending upon the size and the need of the particular business or organization.

<p style="text-align:center">The LDAP Protocol</p>

In terms of the database structure for the digital certificates, this is most useful and effective when the LDAP servers are utilized. LDAP is merely an acronym which stands for "Lightweight Directory Access Protocol", and is simply a database protocol which is used for the updating and searching of the directories which run over the TCP/IP network protocol (this is the network protocol which is primarily used by the PKI Infrastructure for the ZTF).

It is the job of the LDAP server of the Public Key Infrastructure to contain such information and data as it relates to the digital certificates, the public and the private key storage locations, as well as the matching public and private key labels.

The Certificate Authority uses a combination of the end username and the matching tags to specifically locate the digital certificates on the LDAP server. From that point onwards, it is the LDAP server which then checks to see if the requested digital certificate is valid or not, and if it is valid, it then retrieves from its database a digital certificate which can then be sent to the end user. Although all digital certificates which are issued have a finite lifespan when they are first issued, they can also be revoked for any reason at any time by the Public Key Infrastructure Administrator.

In order to accomplish this very specific task, a Certificate Revocation List, or a CRL is used. This list is composed of the digital certificate serial numbers which have been assigned by the Certificate Authority. But, looking at this type of information and data can be very taxing on the system resources and processes.

Therefore, in this regard, it is obviously much easier to reissue the digital certificates as they expire, rather than to revoke them and then having to reissue them again, and of course, which would mean that the Public Key Infrastructure System Administrator would then have to update the Certificate Revocation List.

The PKI Standards

The Public Key Infrastructure is also governed by a body known as the Public Key Cryptography Standards, also known as the PKCS. The bottom line here is that a smooth-running PKI will lead to an efficient and effective Zero Trust Framework. The first of these standards has been previously described, and they are the RSA Encryption Standard, the Diffie-Hellman Key Agreement Standard, and the Elliptical Wave Theory. The other sets of standards which define a Public Key Infrastructure are as follows:

1) The Password Based Cryptography Standard:

   This describes how to encrypt a private key with a secret key which is derived from a password.

2) The Extended Certificate Syntax Standard:

   This is merely a set of attributes attached onto a Digital Certificate which has been assigned by the Certificate Authority.

3) The Cryptographic Message Syntax Standard:

   This standard specifically outlines how to put the digital signatures into digital certificate envelopes, and from there, put that into another digital envelope.

4) The Private Key Information Syntax Standard:

   This standard directly specifies what kind of information and data should be included into a private key, and how that specific key should be formatted.

5) The Selected Attribute Types:

   This is a detailed list which at length describes the certain encryption attribute types for the last three standards;

6) The Certification Request Syntax Standard:

   This provides the details for the syntax for the digital certificates. Essentially, this standard simply sets forth the parameters which are needed for the Certificate Authority to understand the digital certificate request.

7) The Cryptographic Token Interface Standard:

   This is an Application Programming Interface (API) for specifying and handling the cryptographic functions as it relates to the smartcards.

8) The Personal Information Exchange Standard:

This standard specifies exactly how an end user's private keys should be transported across the network medium.

9) The Cryptographic Token Information Format Standard:
   This standard specifies how the applications at a place of business or organization should interface with smart cards.

In the world of Public Key Infrastructure, it should be remembered that the public keys and the private keys (also known as the digital certificates) are created instantaneously and all of the time, whenever the need for access to shared resources is required. In fact, public keys and private keys are everywhere in a Public Key Infrastructure, even when one establishes a Secure Shell (SSH) connection over the Internet with their particular brand of web browser (this typically uses 128-Bit Encryption).

In fact, there are even public keys and private keys in the Public Key Infrastructure which are only used once, terminated, and are literally discarded away. These types of public keys and private keys are known more commonly as "session keys". In the end, digital certificates are nothing more than computer files.

<div align="center">Parameters of Public Keys & Private Keys</div>

But before the actual public key or the private key can go out in the Zero Trust Framework, it needs to have certain parameters which are specified to it, and these are as follows:

1) The type of mathematical algorithm which should be used;
2) How many bits of data the public keys and the private keys should be composed of;
3) The expiration date of both the public keys and the private keys.

Also, in order to keep the hackers at bay, it is equally important that not all of the public keys and the private keys are used all the time in the communication process between the sending and the receiving parties. It is also important to keep the public keys and the private keys fresh, or in other words, it is important to introduce randomness into the Public Key Infrastructure.

Such randomness is known as "Entropy", and this entropy is created by what is known as "Random Number Generators", and "Pseudo-Random Number Generators." Also, in a Public Key Infrastructure, there are different classes of both public keys and private keys. Here is a listing of just some of these classes of keys:

1) Signing Keys:

   These are the keys to creating digital signatures.

2) Authentication Keys:

   These are the keys which are created to authenticate computers, servers, and the receiving parties and the sending parties with one another.

3) Data Encryption Keys:

57

These are the keys which are used to encrypt the files.

4) <u>Session Keys</u>:
These are the types of keys which are used to help secure a channel across an entire network for only a very short period of time.

5) <u>Key Encryption Keys</u>:

These types of keys literally wrap the ciphertext to provide further protection between the sending and the receiving parties.

6) <u>Reof Key</u>:

This is the master which is used for signing all of the other public keys and private keys which originate specifically from the Certificate Authority.

A Review Into Biocryptography

Biocryptography provides the means to further biometric templates at these critical junctures. As it was reviewed chapter 2 of this book, Cryptography is the science of scrambling information and data which is transit across a network medium, and then descrambling it at the receiving end into a decipherable format.

That way, if the scrambled information and data were to be intercepted by a third party, there is not much which can be done unless they possess the keys for descrambling the information. These concepts of scrambling and descrambling can be very easily applied to Biometrics. This is formally known as "BioCryptography".

In other words, the Biometric Templates are protected by scrambling and descrambling keys while they are stored in the database, or in movement across a network to the shared resources server.

To review, whenever we send a message to our intended recipient-whether it is by e-mail, instant message, or even just a text message on our Smartphone, this message is often sent as a "plaintext", or "cleartext".

This means that the actual message is being transmitted to the intended recipient in the way it was originally constructed by the originator of the message. Thus, the only true way to protect the information being sent is to scramble it, in other words, "encrypt the message". This encrypted (or now scrambled message) is now known as the "ciphertext".

The reverse of this process is known as "decryption", with the end result being a readable message to the intended recipient. As all of this relates to Biometrics, the data packet which houses the biometric template (such as the fingerprint or iris recognition template) can be viewed as the plaint text, or as the "Plaintext Biometric Template".

The Cipher Biometric Template

When the fingerprint or iris 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". But other than just doing the above, Biocryptography also has to provide the following three functions in order for it to be truly effective:

1) Authentication:

   The shared resources server of the Plaintext Biometric Template) should be able to, 100%, 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);

3) Nonrepudiation: The sender of the Plaintext Biometric Template should not falsely deny that they have not sent the that particular template originally.

Biocryptography In An MFA For The Zero Trust Framework

Although this has been illustrated and reviewed to a certain extent in earlier parts of this book, we are now at a critical juncture where a detailed examination of how all of this comes together. First, as described, there are three main Biometric modalities that will constitute the MFA methodology for the ZFT. There is a logical flow sequence as to how the end user, or employee will be authenticated in this process. The following illustration summarizes this:

| Fingerprint Recognition | → | Facial Recognition | → | Iris Recognition |
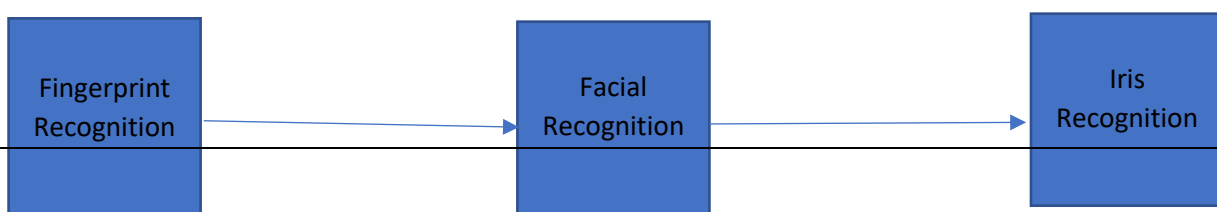
All of these devices will be wired to the authentication server. It is assumed that both the enrollment and verification process will happen in a rapid-fire succession, in perhaps under just a two or minutes. Once this process has been done, all of the Verification Templates will then be scrambled and created to form as to what will be known as the "Cipher Biometric Template". This newly created template will then be further encased into another data packet, for an added measure of protection.

From here, this new template will then be transmitted over to the authentication server so that the end user (or employee) will be granted access to the shared resources that they are seeking to use. In this situation, there are two important points to remember:

1) The newly created Verification Template will actually be a combination of the Fingerprint, Facial, and Iris Recognition Verification Templates. This is what will be sent to the authentication server after this newly created template has been scrambled and encapsulated into another data packet.

2) One of the primary goals is that once the end user (or employee) has been authenticated once, they will not be required to go through this process again. Rather, it is the newly created Verification Template that will be used repeatedly to allow access to the shared resources server. This is where the concept of Privileged Access Management will come into play, and will be further reviewed in detail in Chapter 5 of this book. The ultimate goal here is to create what is known as "One Identity For Life", thus eradicating the use of the password all together.

The process for the newly created Verification Template is illustrated below:
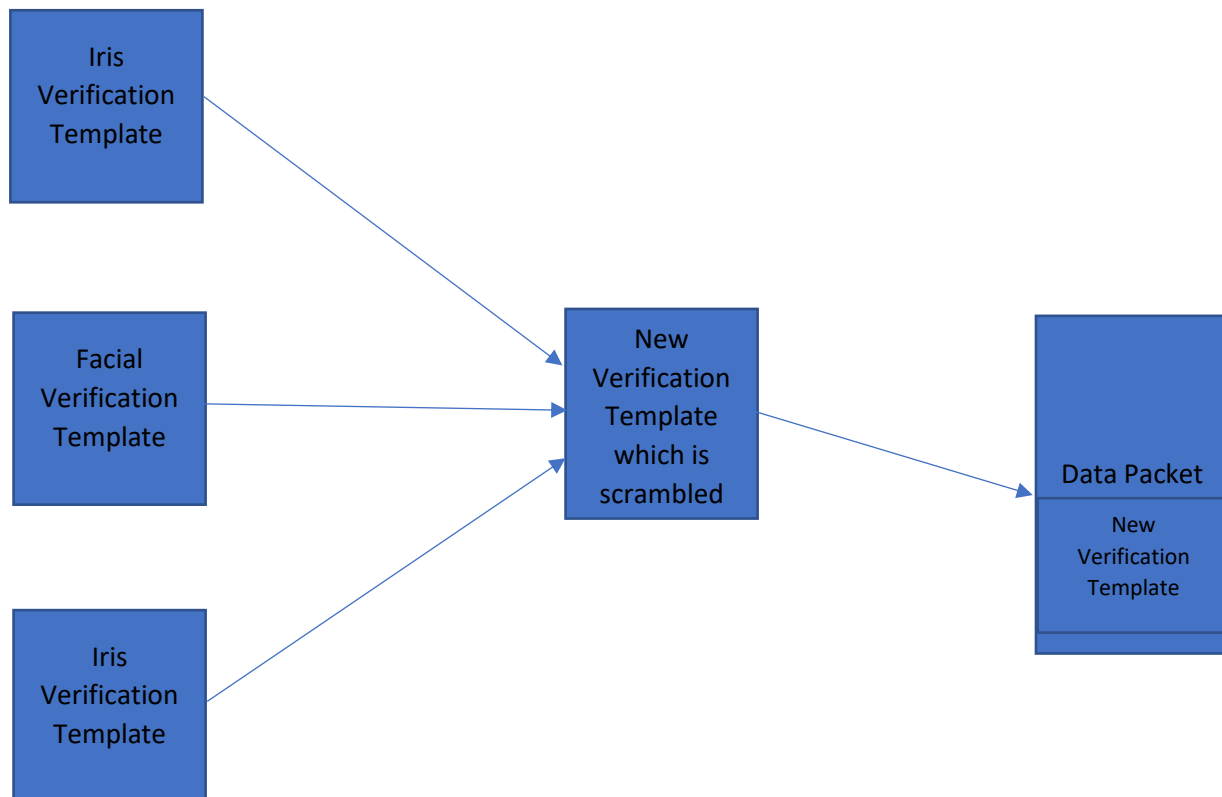
The assumption so far is that the end user (or employee) is that this MFA approach for the Zero Trust Framework is at the physical place of the business location. But given the work dynamics of today's environment, it is also important to address as to how this methodology will work for a remote employee, located hundreds, or perhaps even thousands of miles away.

Biocryptography & Virtual Private Networks

There is yet another tool of BioCryptography which would perfectly here for the Remote Employee– this is known as a "Virtual Private Network", or "VPN" for short.

1) The end user (o employee) has their fingerprint, face, and iris scanned to create the respective verification template. This template then gets broken down into a separate data packet. This data packet (which contains the newly created verification template) is then further encapsulated (or encrypted) into another data packet, so it eventually becomes invisible as it traverses across the various network media, as it makes its way to the servers of the hosting provider;

2) To ensure the integrity of this double layered data packet, it would also consist of headers which contain information about the size and type of the newly created verification template. This would be a confirmation to the shared resources server that this has not been changed en route;

3) To create another layer of protection, a dedicated VPN channel can be created. This would be a direct line from the point of origin of the fingerprint or iris scanner all the way to the servers of the hosting party. This is known as specifically as "IP Tunneling", and as a result, this channel cannot be seen by other people accessing the Internet across the same network media the data packets (which contains the verification templates) are also traveling across;

4) Once this data packet arrives at the shared resources server, it is then decrypted, and the end user (or employee) can then gain access to the resources they need.

The Hashing Mechanism

As it was mentioned in the last section, of the primary goals of the Zero Trust Framework (or at least the way that we are proposing it in this book) is eliminate the need for the end user (or employee) to have be authenticated over and over again. The goal is that they get authenticated once, and that's it. So because of this, the newly created Verification Biometric Template (which can also be referred to as the "Cipher Biometric Template") gets two layers of protection, the first of it being scrambled, and the second, having it encapsulated in second data packet.

But, if the same Verification Template is to be used over and over again, the shared resources needs to have confirmation that this template has not been altered or tampered in away in the transition process. In other words, it has retained its level of integrity, and will need to do so over and over again, until a newer Verification Template has been created.

This is where the Hashing Function comes into use. In simplest terms, it is a mathematical value that is computed at the point of authentication, and is assigned to the data packet that encapsulates the newly created Verification Template. If this value remains the same as it reaches the shared resources server,

61

then one can be assured that the integrity has remained the same. But, if the mathematical is different for any reason, then that will lead to suspicion the Verification Template has been altered.

To fix this major security vulnerability, the newly created Verification Template is combined with a "secret key" at the point of authentication first, then the hash value is created. As a result, this hash will then contain specific information and data about the secret itself. As a result, the shared resourced server can even be further ensured that the Verification Template they have received is one hundred percent original sent by the authentication server.

This is so because even if the Verification Template, the hash, and the associated secret key were to be intercepted, there is very little that a hacker can do to alter the Verification Template. and its associated hash, because they have to have the information and data about the secret key, which is of course something they will never gain access to.

Although the Hashing Mechanism provides for a far greater level of assurance with regards to the integrity of the Verification Template, it is not totally infallible either. Therefore, the use of Quantum Mechanics and Photon Particles, at least in theory, could provide as much as 110% integrity assurances. This will be covered more in Chapter 5 of this book.

The Hashing Function is illustrated below:
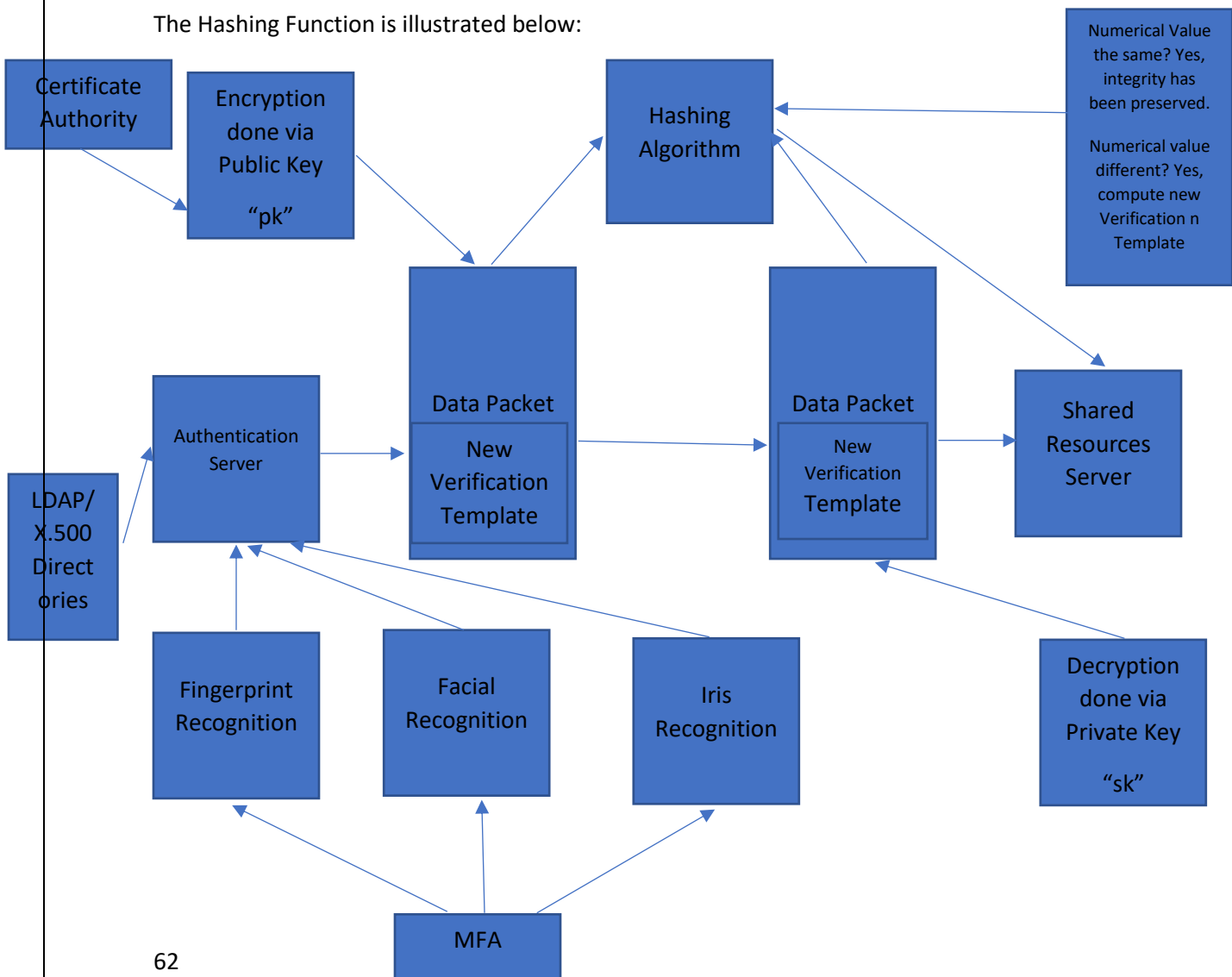
This illustration is reviewed as follows:

1) The end user (or employee is enrolled and verified by MFA, which includes Fingerprint Recognition, Facial Recognition, Iris Recognition.
2) The enrollment template is stored in the database of the Authentication Server (via the LDAP and/or X.500 Directories), and at this point, the end user (or employee) goes through the verification cycle. From here, the first Verification Template is then created. The person in question is fully authenticated.
3) The new Verification Template is a culmination of all three templates after the first verification. It is encapsulated into another data packet, and is encrypted via the Public Key.
4) At the point of authentication, the hashing algorithm and its numerical value is computed.
5) The data packet then makes its way to the shared resources server.
6) It is then decrypted with the Private Key, and access is granted to the end user (or employee) to get to the shared resources that they need to access.
7) Finally, if the numerical value of the Hashing Algorithm remains the same, the Verification Template remains intact. If not, it has been altered, then the entire process has to be repeated again.

CHAPTER 5: Quantum Mechanics And The Zero Trust Framework

Introduction

The first three chapters of this book have reviewed the following topics, which are all very important facets for the development of a Zero Trust Framework:

➢ The basics of Cryptography;
➢ Two Factor Authentication;
➢ Multifactor Authentication;
➢ An examination of the key Biometric modalities that can be used for an MFA approach:
   *Fingerprint Recognition

   *Iris Recognition

   *Facial Recognition.

From this point, the book then segwayed into the fact that a Zero Trust Framework does not have a single user approach, as our previous examples in these chapters demonstrated. Rather, in today's environment, especially in the larger businesses, there will be many end users attempting to gain authentication to many other shared resources, across different servers. Thus, the need to have a Zero Trust Framework that can handle this load is a must.

Thus, the concept of Asymmetric Key Cryptography was introduced, which is also known as a Public Key Infrastructure, or PKI for short. With this newer approach, many end users can be authenticated and authorized to gain access to many shared resources. In of by itself, this kind infrastructure can be resource intense, but in order to streamline this process, other concepts were also introduced:

➢ Public Keys;
➢ Private Keys;
➢ Certificate Authorities;
➢ LDAP/X.500 Directory structures.

It is the Public Key which encrypts the Biometric Template, and the Private Key which decrypts it. The Certificate Authority serves as the central point in which the Digital Certificates (also known as the Public Key and Private Key) are issued. Further, they can be used over again with some alterations made to them at a subsequent point in time, and thus these Digital Certificates are stored in the LDAP/X.500 Directories, which serve as the database.

From here, Chapter 4 then delved into the topic of BioCryptography. This is a new and upcoming area of Cybersecurity, and the basic premise of this concept is to further fortify the strength of the Biometric Templates by encrypting them and further encapsulating them into another data packet. Further, another goal of the Zero Trust Framework is to create what is known as a passwordless organization.

For example, in the context of the Zero Trust Framework model that we have proposed in this book so far, the same Biometric Template can be used over and over again without having the end user (or the employee) go through the same authentication and authorization processes repeatedly. For example, in

the context that we have proposed, an end user (or an employee) would first have to be authenticated by having themselves enrolled first via the three aforementioned Biometric modalities.

These newly created Enrollment Templates can be housed in the LDAP/X.500 Directories, but in order to gain access to the shared resources, the end user (employee) would have to go through another cycle, which will then lead to the creation of the Verification Templates. In the end, it is the Enrollment and the Verification Templates which are compared amongst one another, and if there is a close enough match, then the identity of the end user (employee) is confirmed, and thus, they will be given access to the shared resources server to get access to whatever they are requesting.

But now, imagine having to go through this process each and every time that your employee needs access to shared resources. Not only would it be a very time-consuming process, but the drain of resources and the processing power of our proposed Zero Trust Framework would be immense. Therefore, the goal would be to create the ability to keep using the same templates over and over again. Thus the concepts of Privileged Access Management become critical here.

But, as it was reviewed in the last chapter, these different templates that were created will have to be created into one master template, which would then be sent over to the shared resources server for authorization. Because of this, the integrity of this newly created template is absolutely critical. Thus, the concept of Hashing Algorithms was introduced. But these too are prone to a Cyberattack, and because of that, Quantum Mechanics was introduced as a replacement for it. Finally, Chapter 3 concluded with a diagram of what has been reviewed and proposed up to that point in time for our Zero Trust Framework.

We will go back to this very diagram, and from there, add the other key features to our proposed Zero Trust Framework, which are as follows:

1) Privileged Access Management (PAM);
2) Quantum Mechanics (especially that of Quantum Cryptography);
3) Photon Particles.

But first, since this chapter is about the Zero Trust Framework exclusively, it is important to review its origins and its other major facets, other than the ones we have reviewed so fare in this book.

The Origins Of The Zero Trust Framework

In reality, the concept of the Zero Trust Framework is nothing new. In fact, it dates back more than a decade ago, all the way to 2010. An individual by the name of John Kindervag developed the philosophy that nothing should be trusted at all, from both within the external and internal environments of a company, or for that matter, any type of entity. The motto here was to get rid all of levels of trust, even how slight it may be. The driving philosophy was to "never trust, but always verify, no matter how many times it has to be done".

Although the concept of the Internet of Things (IoT) was not even heard back during those times, people trying to access connected devices could not be trusted, everybody has to go through the same regimen of verification. John Kindervag even related this concept to Joseph Stalin with his famous quote, "I trust no one, not even myself". Eventually, he named his theory the Zero Trust Framework. Thus, as will be elaborated more later in this chapter, the Zero Trust Framework is not a "one size fits all" approach.

This means that whatever works for one entity regarding the ZTF will not work for a different one. Rather, it is a methodology that has to be crafted and molded to the exact and unique security requirements of the company.

Probably the first true commercial application of the Zero Trust Framework came back when the United States Office of Personnel Management was hit by a Cyberattack. The House of Representatives mandated the use of the ZTF methodology in order to safeguard not only their digital assets, but also for the rest of the US Federal Government.

Other notable events in the history of the Zero Trust Framework which has led to its higher levels of adoption today:

<p align="center">In 2011</p>

Google came out with its own version of the Zero Trust Framework, and this was called the "BeyondCorp". The main trigger for this was the Cyberattack known as "Operation Aurora", which was launched in 2009. This was deemed to be an Advanced Persistent Threat (also known as "APT"). The premise behind this model was to do away with network segmentation all together, and instead rely upon the use of Multifactor Authentication (MFA) as the main source for both authentication and authorization. More information about Beyond Corp can be seen at the link below:

https://www.beyondcorp.com/

In 2014, Google published a whitepaper about their proposed framework, which gave a rather big boost to the overall concepts of the Zero Trust Framework. This is deemed to be an important piece of work, and it can be downloaded and viewed at this link:

http://cyberresources.solutions/ZTF_Book/Beyond_Corp.pdf

<p align="center">In 2018</p>

Forrester came up with their own model of the Zero Trust Framework, which was entitled the "Zero Trust eXtended Ecosystem". This methodology consisted of 7 different layers, which are as follows:

- Workforce Security;
- Device Security;
- Workload;
- Network;
- Data Security;
- Visibility and Analytics;
- Automation and Orchestration.

Also, the National Institute of Standards and Technology came out with their own version of the Zero Trust Framework and this was released as Special Publication 800-207. Subsequently in 2020, this publication was updated.

<p align="center">In 2019</p>

Gartner, in a manner similar to that of Forrester, also launched their version of the Zero Trust Framework, which was called the "Zero Trust Network Access" (also known as the "ZTNA"). In return this also gave birth to a new Cyber concept (and even tool) called the "Secure Access Service Edge", also

more commonly known as "SASE". The premise of this is that any processing and transactions of data sets occurs close to the device that is requesting these services, rather than having them done at the central database server.

In 2021

Another major catalyst for the adoption of the Zero Trust Framework was the COVID-19 pandemic. With everybody now working from home, businesses were seeking new ways in which to counter the new threat variants which persisted. In fact, according to a research report which was published by Microsoft entitled the "Zero Trust Adoption Report" an overwhelming 96% of the 1,200 respondents polled said that they favored the concepts of the overall concepts of the Zero Trust Framework.

From 2021 to Present

The Biden Administration has been the main trigger during this time frame, with the following events being the main drivers:

*Executive Order on Improving the Nation's Cybersecurity: This was signed in May 2021, with the main intention of enhancing the security posture of the US Federal Government and the nation's Critical Infrastructure.

*The U.S. Office of Management and Budget (also known as the "OMB") further endorsed the adoption of the Zero Trust Framework.

*The Cybersecurity and Infrastructure Security Agency (also known as the "CISA") also came out with a different version of the Zero Trust Framework, and it was called the "Cloud Security Technical Reference Architecture and Zero Trust Maturity Model". This methodology focused more upon Cloud based security, especially focusing on data leakages, whether intentional or not.

*The Acting Director of the OMB (Shalanda D. Young) gave Federal Agencies until the end of the Fiscal Year of 2024 to deploy and implement certain controls to fulfill the following objectives of their own version of the Zero Trust Framework:

  ➢ Identity;
  ➢ Devices;
  ➢ Networks;
  ➢ Applications and Data.

*The CISA came and published the second version of their Cloud Security/Zero Trust Framework Publication. It can be downloaded and viewed here:

http://cyberresources.solutions/ZTF_Book/CISA_Publication.pdf

*Okta conducted a major market research project which was entitled "The State of Zero Trust Security 2022." It was discovered that at least 72% of all of the Federal Agencies had some sort of Zero Trust plan in place, or they were at least working on the first drafts of one.

(SOURCE: https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security)

The origins of the Zero Trust Framework can be summarized in the illustration below:

67

A whitepaper is published by Digital Equipment Corporation discussing how Firewalls can be used in a segmented Network Infrastructure, in 1987

↓

The concept of Virtual LANS (vLANS) is used is introduced into the first segmented networks, in the early 1990's.

↓

The IEEE Standards Association creates and publishes the 801.X protocol for Network Access Control (NAC) in 2001. The NAC is a component of the Zero Trust Framework.

↓

The Jerico Forum is established, and introduces the first concepts of "deperimeterization" in 2004.

↓

The first concept of the Zero Trust Framework is introduced by John Kindervag, in a whitepaper published in 2010.

↓

The BeyondCorp model from Google is born, in 2014.

↓

Zscaler creates the first Zero Trust Framework for a Cloud based Architecture, in 2016.

↓

Gartner comes into the Zero Trust Framework with its concepts of the SASE, in 2019.

↓

The NIST comes into the Zero Trust Framework with its SP 800-207 publication, in 2021.

↓

Gartner reveals another Zero Trust Framework, in 2021.

↓

The US Government starts to mandate the Zero Trust Framework, in 2022.

For the longest time, businesses have adopted what is known as "Perimeter Security". A technical definition for it is as follows:

"Perimeter security is the philosophy of setting up functional apparatus or techniques at the perimeter of the network to secure data and resources."

(SOURCE: https://www.techopedia.com/definition/33764/perimeter-security).

In other words, imagine one large circle encompassing a business, which is the main line of defense. That can be thought of as Perimeter Security. It is from within the confines of this circle that a business will deploy all of the firewalls, network intrusion devices, routers, etc. as well as other types of security technologies in order to fortify their defenses. It is also at this point that the authentication mechanisms will be deployed, especially from the standpoint of Physical Access Entry. This is illustrated in the diagram below:
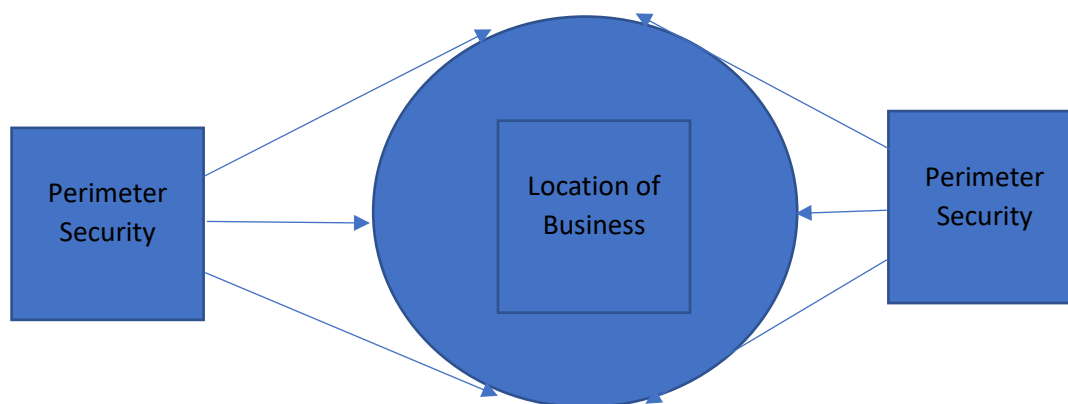
With this kind of approach to security, there was always an implicit level of trust that was recognized. For example, if you were an employee gaining access to shared resources, it was always assumed that you went through all of the authentication processes that were in place. Even if you were a third-party vendor the vetting process was very easy and simple to get through, because there was an implicit layer of trust that no intentional harm would ever be done to the data sets or the business processes that were being outsourced. In other words, the main concern was protecting the organization from threats that were coming from the external environment.

Nobody was really ever concerned about the internal environment of the business, because after all, once again, if you were an employee, nobody really paid too much attention to your specific rights, permissions, and privileges. It was always assumed you were given the right amount to do your daily job tasks. Because of this, the thoughts of an Insider Attack from precipitating was pretty much null.

But there is one major problem with the Perimeter Security approach. This is model assumes only layer of security. Thus, if the Cyberattacker were to penetrate through it, you then have pretty much given away the keys to the crown jewels of your company, because there are no other layers of security located from within the confines of the business.

There are other reasons for the eventual erosion of the Perimeter Security model, which are as follows:

69

1) <u>The Remote Workforce</u>:
   Many people thought that a 100% Remote Workforce would transpire later this decade. But instead, the COVID-19 pandemic made this into a reality within just a three-month timespan. With the influx of workers now working from home, there were many security issues that transpired. One of the largest ones was the intermingling of both the corporate network with the home-based networks. Goen were the days where an employee could simply log into their workstation with their username and password. Now, with two different types of network infrastructures touching base with another, remote employees now absolutely had to be confirmed with more than just one layer of authentication. As a result, many IT Security teams were left scrambling to implement a system where at least two or more layers of authentication would be required. This proved to be a major catalyst for the companies to start at least thinking about deploying the Zero Trust Framework in a serious manner.

2) <u>The breakdown of the Virtual Private Network (VPN)</u>:
   The VPN before the COVID-19 pandemic hit always provided a secure way for employees to remotely login into the servers where the shared resources were held. But during these times, only about 25%-30% of employees were actually working remotely. But with the rapid influx to a near 99% Remote Workforce, the VPN started to show its breaking points. As a result, the Cyberattacker was able to exploit new weaknesses in a legacy system. Once again, using two or more layers of authentication and the concept of "Never Trust, Always Verify" took even further hold.

3) <u>The race to the Cloud</u>:
   Along with the issue of the intermingling of corporate and home-based networks, many remote employees were given company issued devices that were not properly fitted with adequate security protocols installed onto them. Because of this, and other reasons, many businesses started to migrate their On Premises Infrastructures into the major Cloud based platforms, such as that of the AWS and Microsoft Azure. Since this was an unknown territory for many organizations, especially for the SMBs, many of them chose to utilize the Private Cloud deployment because of the security that was afforded. But as familiarity with the Cloud started to settle in, many of them subsequently started to move out to the Hybrid Cloud model. This is essentially a combination of the Private Cloud and Public Cloud. But since lines access and separation were not too clear, many login credentials became at risk here, as the IT Security teams struggled to keep track which end user (or employee) accounts needed to be created, and those which had to be deleted and/or deprovisioned. Even to this day this is a big problem, as data leakage issues have emerged, especially with the AWS S3 buckets. This is an area now in which the IT Security teams are starting to realize which needs much more attention, especially through the use of automation. The use of Privileged Access Management (PAM) in a Zero Trust Framework is a solution, and as mentioned earlier, it will be explored in more detail later in this chapter.

4) <u>Artificial Intelligence (AI) and Machine Learning (ML)</u>:
   The last couple of years have seen a huge rise in both of these technologies, especially when it comes to automation. This concept just does not apply to manufacturing scenarios (this is where Robotic Process Automation comes into play), but it can also apply to virtual processes as well, such as when it comes to optimizing and parsing through large datasets (which is also

known as "Big Data"). For example if there is one Virtual Machine (VM) which has SQL Server running and another VM that is running an Oracle Enterprise database, and they both are conducting automated tasks, there cannot be any kind of accidental data interchange between the two servers. Thus, only a Zero Trust Framework can help prevent this from happening, as these VMs be segregated from one another by their own boundaries.

The Demise of Perimeter Security

In the end, the ultimate goal of Perimeter Security was to keep all assets, whether they were digital, physical, or intellectual within the confines of the business, and the Perimeter Defense would contain them there, and provide protection under just one layer of security. But given the reasons in the last subsection, as well as other factors (such as the rise of Insider Attacks and the overwhelming amount of threat variants from the external environment constantly pounding it), the demise of Perimeter Security finally happened.

Now, with offices and employees around the world and working in a virtual-based environment, the Perimeter Security Model will no longer suffice. This scattering of assets and resources for a company can be seen below:
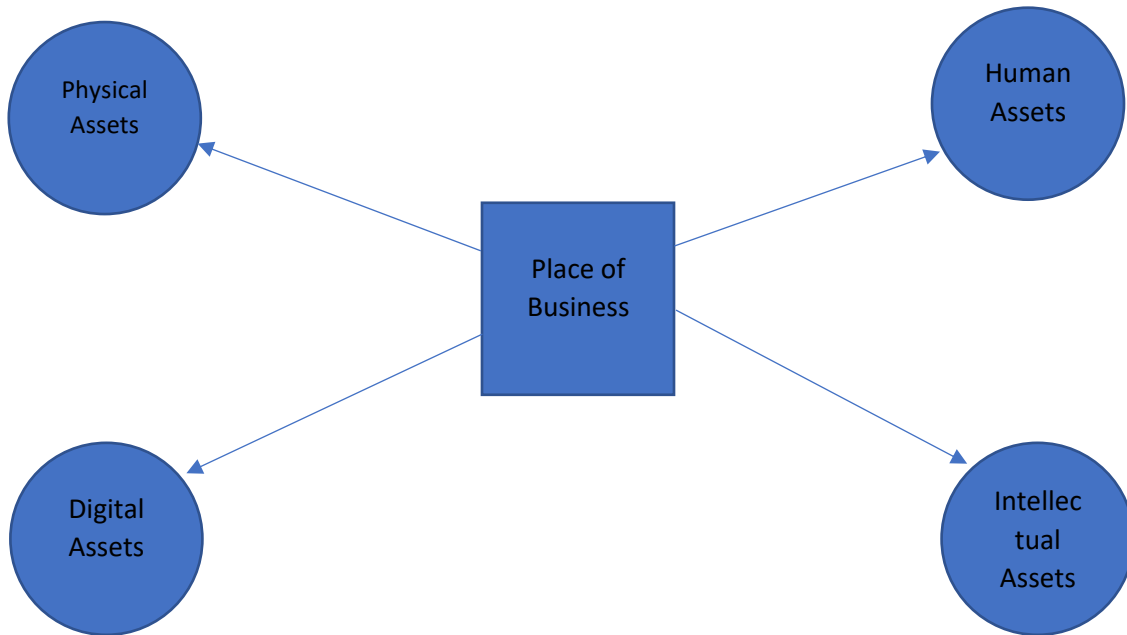
As a result, since everything is scattered all over the world, no kind of trust cannot be afforded anymore, thus fueling the demand for the Zero Trust Framework even more.

The Emergence Of The Zero Trust Framework

So far in this chapter, we have provided a history of the evolution of the Zero Trust Framework, and reviewed the factors that led to the eventual demise (or almost near collapse) of the Perimeter Security Model. Thus going forward, we now assume that the Zero Trust Framework will be the methodology of choice for not only keeping the IT and Network infrastructure secure for an organization, but is also one the most optimal ways in the authentication and authorization for end users (or employees) to gain access to shared resources, and other types of confidential assets.

Before we resume with the initial Zero Trust Framework model, we introduced at the end of Chapter 4, it is important some of the key properties of what truly makes up this framework. Some of these are as follows:

1) <u>It depends on risk</u>:
   Theoretically speaking, you want to protect everything that is at risk in your business. But in a real-world sense, we know that this is totally infeasible. You can only give the highest levels of protection to those assets that are the most vulnerable to a security breach. Now, the question arises as to how to decide what is weak? One of the best ways to figure this out is for you and your IT Security team to take an inventory of all of the assets that your company has (both digital and physical), and break them down into the different categories that they belong to. Once this has been completed, you can then rank them on a scale, perhaps where 1 = Least Vulnerable and 10 = Most Vulnerable. Anything in the intermediate range would get a medium ranking. Now, you take all of those assets and from there determine the appropriate controls that they need.   The bottom line here is that the depth of your Zero Trust Framework will be dependent upon how many vulnerable assets you have, and how much they worth that they have for the organization. Meaning if you have a lot of them, you will need to break out your IT and Network Infrastructure into more, smaller units. But if you are a smaller business, you may not have as many assets on hand, thus the need for segmentation will not be as high, and you will have a lesser number of units that need to be divided.

2) <u>Repeated use fo MFA</u>:
   A constant theme throughout this book, especially in Chapters 3 and 4, has been the use repeated use of Multifactor Authentication. For each and everything you need to access to, you must keep getting reauthenticated and reauthorized. This is also a core element of the Zero Trust Framework. While once again in theory this is probably the best way to fortify you lines of defense, following this procedure in the real world could prove to be very ineffective. For example, in the Public Key Infrastructure (PKI) methodology that we have proposed, there will be an enormous drain on both resources and processing power. Therefore, one of the goals of is to introduce Privileged Access Management (also known as "PAM") which will allow for the end user (or employee) to have to through the entire authentication and authorization only once. This will also be reviewed in greater detail later in this chapter.

3) <u>Endpoints are further protected</u>:
   One of the major pitfalls of the Perimeter Security Model is that the Endpoint Security has often been a forgotten topic. Essentially, the endpoints are the points of origination and termination

for the network lines of communication. Since they have been ignored for such a long period of time, this has been a favorite point of entry for the Cyberattacker to penetrate into an IT and Network Infrastructure. As a result, they have been able to stay in for long periods of time, and move laterally in a covert fashion. Because of this, they also have been to exfiltrate data a bit at a time, very often going unnoticed, until it was too late. But, of the strategic advantages of the Zero Trust Framework is that this is no longer an issue. In other words, Endpoint Security is a very crucial component that cannot be forgotten about.

4) Isolation:
   With the Perimeter Defense model, not only was it much easier for a Cyberattacker to get in, but it was also easier for them to get out of the system if they were detected. But this is not the case with the Zero Trust Framework. Because the IT and Network Infrastructure is broken up into different segments, it makes that much more difficult for the Cyberattacker to get through the crown jewels of the organization. But by the time he or she has broken through any lines of defense, the IT Security team will have alerted, and remediative action would have followed immediately. Thus, there are very good chances that the Cyberattacker will be isolated with no point of exit possible.

5) Finer levels of control:
   Under Perimeter Defense, for the most part, the concept of Least Privilege was followed. But most of the rights, permissions, and privileges were of a "macro" one, meaning that it was quite possible for an end user (or employee) to still access other applications when they had no reason to. In other words, people were put into various groups and profiles into an Active Directory structure with the rights, permissions, and privileges already pre-established into it. There were no finer controls established to prevent unintended access to other systems. This becomes especially crucial for Privileged Accounts. Thus, another key mandate of the Zero Trust Framework is to establish a granular (or finer) set of controls that will eliminate this kind of crossover to other applications.

6) Comprehensive Auditing:
   Most companies set up their Perimeter Security to only audit certain parts of their It and IT Network Infrastructures. Most of them were set up to only monitor the flow of network traffic in and out of the business, and to detect any rouge data packets. It wasn't until recently that the interest of detecting malicious or unusual behavior picked up, with the advent of both AI and ML tools. But with the Zero Trust Framework, and especially for those deployed in a Cloud based environment, there are now tools available that give the IT Security team the ability to audit everything in their respective infrastructures. This also includes the ever-important endpoints, and even the ability to track a wireless device on a real time basis, and even obtain a log file from that. Also with Perimeter Defense, the IT Security team traditionally had to comb through all of the log files that were outputted on a manual basis. Compounding this fact was that security tools came from different vendors, and as a result of that, different formats were created. But now, and with the growth of the Zero Trust Framework, a central console can be used (which is a Security Incident Event Manager, or "SIEM" for short) to see the outputs of all of the log files from one central location.

7) The use of Adaptive Control:

The common way to detect any sort of malicious or rogue behavior under the Perimeter Security Model was to create a simple baseline and from there, upon the thresholds set by the IT Security team, anything outside of what was deemed to be normal would require further attention. But this would often trigger what are known as "false positives". In order to alleviate this situation, there are other variables that have to be taken into account in order to determine true, rogue behavior. These are as follows:

*Time of the day;

*Day of the week;

*Geographic location;

*IP Address;

*Target Server;

*Target Application.

These kinds of specifications are more or less required by a Zero Trust Framework, and to be conducted on a real time basis. The variables just examined above are also technically known as "Adaptive Controls".

8) Contextual Request:
   With implicit trust being used in a Perimeter Defense Model, any elevation of privileges, rights, and permissions were often granted without a second thought, especially for the privileged accounts. But since the Zero Trust Framework means absolutely no trust whatsoever, the granting of super user permissions can only take place if only questions such as the entity who is requesting this, the target server, why this kind of access is needed, and for how long it will be required have all been answered.

9) Lateral Movement:
   Since there are many layers of security in the Zero Trust Framework, the lateral movement of a Cyberattacker is almost nil after even penetrating the first one or two layers. This is unlike the Perimeter Defense Model, while after piercing through the first and only line of defense, the Cyberattacker will have complete reign in the IT and Network Infrastructure.

The Basic Zero Trust Framework Model

Now that we have reviewed some of the most properties of the Zero Trust Framework, it is now at this point we into actually present the basic model of the Zero Trust Framework. Once again, keep that this is a methodology, and it is not meant to be a cookie cutter approach to security. Businesses can modify it by making additions to it as they see necessary.

<u>The Model</u>
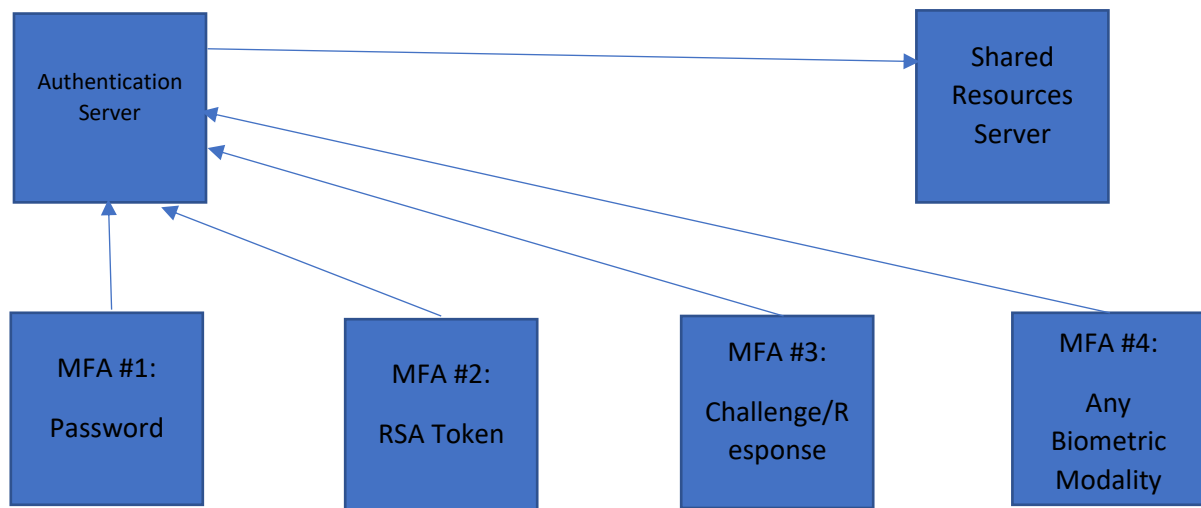
This can be deemed to be the most fundamental model of the Zero Trust Framework. For example, the first embraces Multifactor Authentication (MFA), in which at least three more mechanisms are used. In the scenario above there are four of them, and there are three types of identification criterion that are met in this case, which are as follows:

1) <u>Something you are</u>:
    This is typically something that is permanent about your, such as your physiological or behavioral self. This is where Biometrics (reviewed in Chapter 3) will come into play (which is MFA #4).

2) <u>Something you know</u>:
    This is a piece of information and/or data that you know of. It can be a password, an answer to a challenge/response question, etc. These are represented as MFA #1, and MFA #3, respectively.

3) <u>Something you have</u>:
    This is something in your position such as an RSA Token, smart card, FOB, etc. This is represented as MFA #2.

75

Once the end user (or employee) has gone through all of these iterations, he or she will then be granted access to whatever shared resources they need to conduct their daily job tasks. But the caveat here is that each the end user wants to gain access to something else or different, they have to go through this entire process once again. And, if this happens multiple times in a single day (which is highly probable) then it will not only be a cumbersome process, but it can be a drain of processing power on part of the Authentication Server.

In our proposed model of the Zero Trust Framework, we theoretically do away with this repetitive cycle by making use of the concepts of Privileged Access Management (PAM). As mentioned, this will be reviewed in more detail later in this chapter.

Because of the almost near eradication of the Perimeter Defense Model, this has left many businesses in what is called as an "amorphous state". Meaning, there are no clear-cut boundaries as to where all of the digital assets now lie at; they are now technically speaking in different physical locations, but virtually, they look like they are all in one place, if you are using a Cloud based deployment. This now gives rise to a very important concept for the traditional Zer Trust Framework Model: Segmentation.

<p align="center">What Is Segmentation?</p>

When one thinks of this concept, the image of a large unit being broken into smaller bits often comes to mind. This is true of the Zero Trust Framework. A technical definition of Segmentation is as follows:

"It is a network security technique that divides a network into smaller, distinct sub-networks that enable network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network.

The process of network segmentation involves partitioning a physical network into different logical sub-networks. Once the network has been subdivided into smaller more manageable units, controls are applied to the individual, compartmentalized segments."

(SOURCE: https://www.vmware.com/topics/glossary/content/network-segmentation.html).

Although the entire processes and operation of a business can be broken into smaller units or segments, it is typically the IT and Network Infrastructure that is broken down, because it is deemed to be the most vital component (or "heart and soul") of any enterprise. So now, imagine all of those digital assets (this can be everything from the data bases to the Virtual Machines to the Virtual Desktops to all of the datasets, etc.) that are now in existence in any kind of Cloud deployment (again, they are the Private, Public and Hybrid Clouds).

Per the permutations and requirements that have been set forth by the IT Security team and the CISO, all of them now will reside into smaller units, or what will now be termed as "Segments". Each of these segments will be surrounded by their own boundary, with all of the authentication mechanisms which support the MFA protocols. In more technical terms, these can also be referred to as "Subnets", as eluded to in the previous definition. These Segments can still be, on a theoretical level, broken down into smaller ones, which become known as "Microsegments".

It is important to note at this point that this model of the Zero Trust Framework (and even those going forward) require that the authentication methods that are being used **_be different from one another._** This means that for each boundary that encompasses a certain Segment, all the MFA mechanisms used

must be totally different from one another. For example, one could still be a password, one can be a smart card, and the other be Biometric.

But the only caveat here is that there are a finite number of authentication mechanisms that can go around. But even with this, there are still quite a number of possibilities in which you can set up your MFA strategies. For example you could take the MFA from one layer and use them three layers up or down in the segmented IT/Network Infrastructure. Also, the Zero Trust Framework mandates that the same authentication methods for supporting the MFA should not be used for long periods of time. They once again should follow a regular schedule of randomization by swapping them out to a pre-established plan.

Probably the to most important keywords to remember with the Zero Trust Framework are that of Trajectory and Isolation. With the former, even though the Cyberattacker might be able to break through one or two, and perhaps even three layers of defense, the chances of him or her getting to the proverbial crown jewels become almost statistically nil. With the latter, once a Cyberattacker has broken though, the chances of him or her breaking out again are also almost nil again, because they will be facing the issue of Isolation because of the other layers of defense that will be surrounding them.

The illustration below gives a 3-Dimensional of what Segmentation looks like, especially in the highlighted areas:
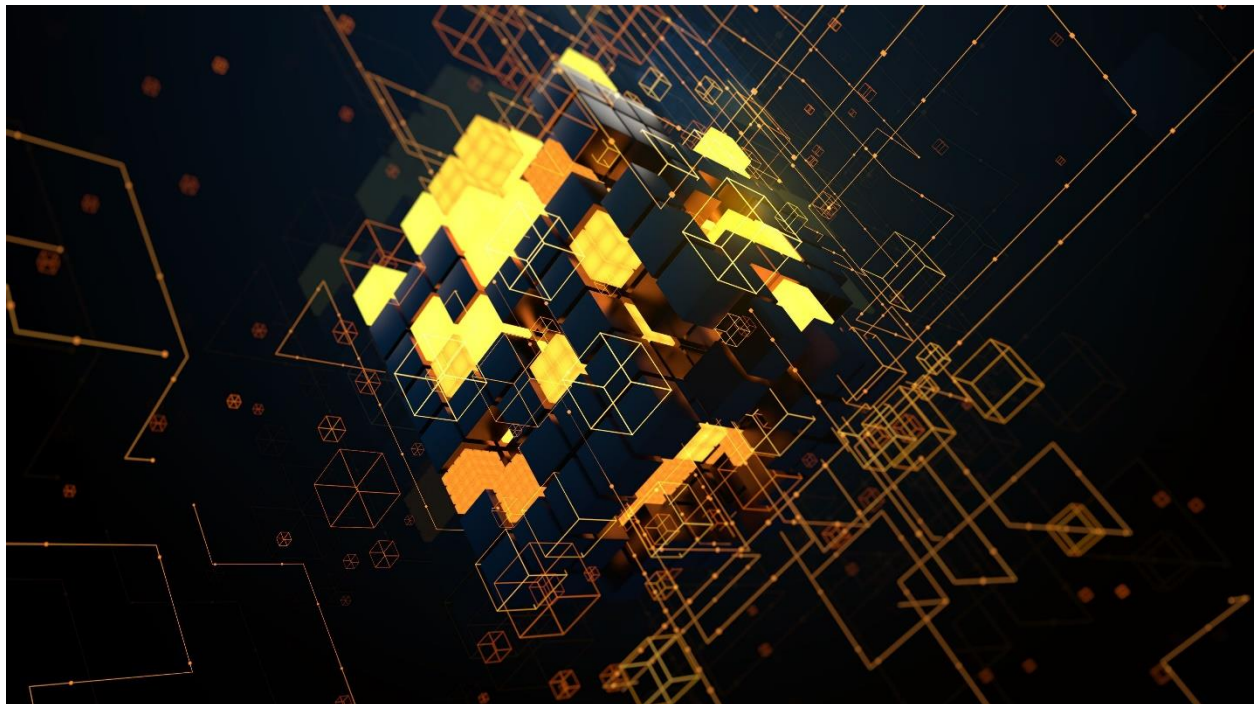
But, this basic model of the Zero Trust Framework does not include the following components of our proposed model, which include the following:

1) The Public Key Infrastructure;
2) Privileged Access Management;
3) BioCryptography;
4) Quantum Mechanics.

As mentioned previously, these above four components will be examined in more detail towards the end of this chapter. But while we are still on this theme of the basic Zero Trust Framework model, the next sections of this chapter will cover the following topics:

➢ The advantages/disadvantages of the Zero Trust Framework;
➢ Best practices in deploying a basic Zero Trust Framework Model at your business.

The Advantages Of The Zero Trust Framework

Although the basic model of the Zero Trust Framework may sound very complex in nature because of all of the Segmenting that will be going on, and all of the MFA authentication mechanisms that will be deployed, once it is established, it won't appear to be that way. But the key here is that whatever Zero Trust Framework Model you deploy, it will have to be deployed in phases. It simply cannot be implemented all at once, as grave mistakes are sure to happen.

In fact, there will be a section later in this chapter that will outline some of the best practices that you can take to deploy the basic model of the Zero Trust Framework. But despite how complex it may look from the outset, there are a number of key advantages that will far outweigh even the ones that are found with the Perimeter Defense Model. Here are some of benefits of the Zero Trust Framework:

1) <u>Both kinds of threats are mitigated</u>:
   By this, we mean the threats from both the external and internal environments. While the Perimeter Defense Model can do a suffice job with the former for a period of time, it does not offer a means by which threats from the internal environment can be tracked. By this, we mean the Insider Attacks. This kind of threat vector can stem from any kind of source, but the common denominator here is that it usually takes an employee from the inside to launch this kind of attack. After all, he or she knows best the internal workings of a company (this depends on their specific job role), and they will of course have some idea as to where the damage can be initiated. For example, this can be an employee who feels that they are about to lose their job, or through a Social Engineering tactic, there could be somebody from the outside world conning an employee to launch such a threat vector. Under the traditional security practices, it is very difficult to detect the beginning of an Insider Attack. At best, the log files will alert the IT Security team of unusual behavior, but this is really not enough to tell with accuracy if anything is about to happen. But with the Zero Trust Framework, the key here is not to only protect from threat vectors that are posed from the external environments, ***but those that are internal as well.*** Given all the internal boundaries, and the many authentication mechanisms, it will be a lot easier now to detect the precipitation of an Insider Attack. In other words, with the Zero Trust Framework, the business is protected from all kinds of environments, which is a huge advantage to have.

2) <u>Can see all of the actions</u>:
   Before the COVID-19 pandemic hit, a lot of the IT Security teams did not pay too much attention to the kinds of types of devices that the employees were using, although they should have been. But once it happened, the fears then quickly arose about who was accessing what through which device, driven primarily because of the intermeshing of both the business and home

networks. Another trigger point for this Bring Your Own Device (BYOD), where remote employees were very often using their own personal device to conduct their daily job tasks, rather than making use of the company issued equipment. With the Zero Trust Framework, a much closer eye can be kept on the devices that are being used to access the shared resources. This is so because each device must now be registered with the IT Security team, and since now MFA will be used, it will be much more difficult for employees to access anything through their personal devices. Also, since all network-based activities can be seen through a central console, the IT Security team will now be able to track down lost or stolen devices, and from that point issue a "Remote Wipe" command to permanently delete any confidential information or data that may have been stored on it. Remember that in the end,

3) Reduction in data loss:
This has always been an issue, even before the COVID-19 pandemic hit. But once it was completely unleashed, the issue of data leakage, whether intentional or not, became a much graver concern. For example, most of the home networks that were being used to access the business network were only using a password as the primary means of defense. This constituted for a weak defense, at best. As a result, the Cyberattacker could very easily have broken though this line of access, and moved laterally into the business network. From here, depending upon where they were at, they could then stay in long enough to see where the datasets reside at, and which ones were the most valuable to exfiltrate. Of course, they are not going to do all of this at once, they are going to take out these datasets a bit at a time, to go unnoticed. But if the Zero Trust Framework had been implemented during this time frame, the fear of data loss would have been greatly diminished, because of all of the layers of defenses that the Cyberattacker would have to literally go through. Plus, each defense layer will also have its own set of controls, thus making data loss/exfiltration an almost impossible task to accomplish.

4) Security is better at the Cloud:
As it has been mentioned throughout this book, many organizations have been moving to the Cloud, and migrating their On Prem infrastructure totally into it. Not only does it afford monthly pricing, but one of the key strategies is that it is highly scalable. For example, if you do have a Zero Trust Framework that is in the Cloud, it is quite easy to break out new assets into their own distinctive segments, as well as deploying the appropriate MFA protocols and authentication mechanisms into place. If for some reason any assets have to be deleted or deprovisioned, the Zero Trust Framework will adjust accordingly, on an automatic basis without any human intervention involved. Also, the major Cloud Providers, especially that of Microsoft Azure, already has a suite of MFA tools that can be installed and deployed with just a few clicks of the mouse. However, it should be noted that the debate between having a Zero Trust Framework in the Cloud versus it being On Premises will always be a continuing one. But making changes to it with the latter will obviously take longer, which is something no organization can afford. Thus, the choice is quite clear in this regard.

5) A newer type of Workforce Model:
The workforce when the COVID-19 pandemic hit was almost all remote based. This meant that people could work from anywhere, in their homes, or even in any other public location, as long as there was a secure Internet connection. But, as the pandemic started to ease down, many

businesses started to reopen their doors. However, a majority of the remote employees preferred to work from the physical location of their office only a few days a week. Thus, this gave birth to a newer type of workforce model, called the "Hybrid Model", where the remote worker would spend one or two days in the office, and the rest of the time would be spent working from home. Because of this, many of these businesses then transferred their Cloud deployment to Hybrid one as well. With this kind of approach, if a Perimeter Defense Model were to be used, it would be much more difficult to keep track of all of where all of the devices were being used at, and which end user (or employee) was accessing which shared resources. But by using the Cloud, the Zero Trust Framework can easily keep track of these geographically separated devices, and ensure that MFA is still being used on them. But the only issue here is keeping track of all of the accounts and profiles in the Azure Activity Directory. But this is where the role of Privileged Access Management (PAM) will come into play.

6) <u>Supports compliance across the board</u>:
The world today is filled with various data privacy laws. Some of the most well-known ones are those of the GDPR, the CCPA, and HIPAA. Depending upon their revenue and employee size, companies will have to come under the tight scrutinization of regulators from each of these laws. If the right controls are not in place, or there are any data leakage issues, the company will be cross hairs for an audit and possible steep financial penalties. But with the Zero Trust Framework, since there are so many controls and authentication mechanisms put into place (especially if you are using a Cloud based deployment), there is a much greater chance that you will more or less be in compliance with these various data privacy laws, and experience a much lower risk of data exfiltration issues.

The Disadvantages Of The Zero Trust Framework

Despite the strategic advantages that the Zero Trust Framework brings to an organization, it also has its set of disadvantages as well. Some of these include the following:

1) <u>It is viewed as extreme</u>:
To an end user (or an employee), The Zero Trust Framework is often perceived as going way too far to the other extreme in security. But unfortunately, despite all of the best efforts to provide employees with security awareness training and trying to keep up with the Cyber Threat landscape, there is really no other choice. There is a lot at stake here for the CISO, as well as other members of the C-Suite and even the Board of Directors, which are namely the protection of the digital assets and the confidential datasets of both the employees and customers. The situation of Zero Trust has been for a lack of a better term, forced upon us, given the dynamics that we are facing today. We simply cannot take anything for granted anymore, because the Cyberattacker has also become a lot stealthier and covert in the way they launch their threat vectors. Some of the people that will feel the worst brunt of the Zero Trust Framework will be those that have been around the longest in a company. Given their long tenure, there is obviously a lot of trust that has been placed with them. But to have that taken all that taken away at once and then not trust them at all (from the standpoint of authentication and authorization) can be traumatic. Therefore, one of the key aspects when deploying a Zero Trust Framework is to keep a direct line of communications open with the end users (or employees) and all levels of management, and vice versa. It is very important to get their buy in even to the

slightest degree possible, and explain the benefits of what it is all about. If this is not done properly, resentment towards the Zero Trust Framework will get even worse, and your end users (or employees) may try to circumvent the system all together, thus defeating its very purpose. One way to alleviate this situation is to deploy your Zero Trust Framework in phases, as was pointed out to earlier in this chapter. By taking this kind of approach, you will be giving your end users (or employees) a time period to digest the new changes that will be happening to them. Although it may take a lot longer to completely build out your Zero Trust Framework to its entirety, the slower the pace the better, at least from the standpoint of end user (or employee) adoption.

2) The use of Micro Segmentation:
As was explained in great detail, the use of the Zero Trust Framework relies heavily upon the concept of Segmentation. Once again, this is where the entire IT and Network Infrastructure is divided up into separate segments, with each of them being surrounded by its own boundary, and MFA authentication tools. But if the organization is a very large one, and if the Zero Trust Framework has proven to be successful, the CISO and the IT Security team could consider making use of what is known as "Micro segmentation". This is where the given Segment is broken down yet into an even smaller one. A benefit if this of course is an extra added layer of security. But if it is deployed for no other reason, it can cause more complication to an already existing Zero Trust Framework. Therefore, any other major tweaks or adjustments like this should only be made if there is some success that has been proven with it initially. In other words, don't add any more to your Zero Trust Framework until it has given you a positive ROI for the time and money you have spent on it initially.

3) A mix of environments:
Although many organizations have made their full shift to the Cloud, there are still some out there that are hesitant to do this, so they have resorted to what is known as a "Mixed Model". This is where they may use part of the Cloud for some of their IT and Network Infrastructure, and the rest still remains On Prem. While this approach may work for some time, it is certainly not a suitable one for the Zero Trust Framework. In other words, it can't be deployed half in one environment and half in another kind. It has to be implemented fully, and in only one type of environment. One of the reasons for this is that it will be a lot harder to keep track of all of the MFA mechanisms that are in place, as well as of the accesses that are being made to the shared resources. Therefore, before even starting to deploy a Zero Trust Framework, you as the CISO, and your IT Security team need to assess the best kind of environment a Zero Trust Framework will work for you. Then you need to plan accordingly. But, if there are any lingering thoughts about making a full migration to the Cloud, you should do that first, then consider the creation of a Zero Trust Framework. But it is also important to keep in mind that a Zero Trust Framework may not even be a viable solution for some businesses, especially those that are classified as a "Small Business" (around 15 employees or less). In these cases, perhaps just using a Two Factor Authentication (2FA) could work as well too.

4) Some flexibility is required:
Although the Zero Trust Framework is inherently designed to be a tight knit kind of environment, there may be some degree of flexibility that is needed in the initial outlay of it, as your end users (or employees) are starting to get used to a brand-new way of accessing

resources that they need. But you and your IT Security team should not let your guard down, as this could be pivotal moment for the Cyberattacker to penetrate into walls of defenses. But even after this, depending upon the job roles that your remote employees have, there may be a need for some flexibility. This will be especially true for those that are deemed to be the "Road Warriors", and need access to applications and/or resources they need immediately to which they never had before.

5) The IoT:
   This is an acronym that stands for the "Internet of Things". Essentially, this is where all of the objects that we interact with in both the physical and digital worlds are all interconnected together. While the IoT has a certain number of key advantages for personal applications (such as the "Smart home", the "Smart Car", etc.), it can pose a serious threat to business applications and processes, and even to the Zero Trust Framework. The primary reason for this is that many of the interconnections in the world of the IoT are often insecure, as they remain unencrypted. In other words, any communications that take place between devices, and any authentication/authorization credentials (such as your username/password, PIN number, etc.). is sent as a "Cleartext", which is decipherable to anybody. If this were to be intercepted by a malicious third party, just about anything disastrous can happen. Also, if any of these IoT devices were connected to a Zero Trust Framework without any prior authorization from the IT Security team, this could yet be another avenue for the Cyberattacker to get in, at least through the first layer of defense.

Now that we have reviewed some of the key advantages and disadvantages of the Zero Trust Framework, we now turn our attention over to a set of best practices that should be at least taken into consideration when deploying the basic model of it.

Some Of The Best Practices

Although the Zero Trust Framework model we have been reviewing thus far in this chapter has been the basic one, there are still a number of key points to keep in mind when you deploy it. Also remember that this methodology is not designed to be a "one size fits all". Meaning what will work for one environment will not work for yours. As mentioned, a lot will depend upon the Risk Assessment that you and your IT Security team have compiled at a previous point in time, and the appropriate set of controls you have decided upon as a result.

Here are some of these key tips:

1) Form a Zero Trust Team:
   Before you even start to draft out a plan for deploying the Zero Trust Framework at your organization, you first need to create a team with the key stakeholders in mind. Obviously, this will consist of you, the CISO, and a representative member of the IT Security team. Keep in mind that this is a methodology which will have an impact on everybody in the business. Therefore, it would be best to also include a representative from the other departments as well. Perhaps even consider including a member of the C-Suite, and the IT Department as well. The purpose of this team is to address all of the concerns and needs of the organization, and how you plan to start the buy-in process for the other employees. Although in theory the Zero Trust Framework

in theory can be used by any business, in practicality, it may not be the most suitable approach for a business. Therefore, this is something that should be discussed as well before moving forward. Also, the impact of a Zero Trust Framework on the technological components and the digital assets that your organization has needs to be taken into very serious consideration as well. But this is a more urgent matter if you still have the On Premises Infrastructure. If you have a Cloud based deployment, then this topic may not be as important to discuss, as templates and strategies should be available to you from your Cloud Provider in guiding you with this process.

2) Assess the environments that you are in:
   By this, if you are 100% in the Cloud, you need and your IT Security team need to take a very accurate stock of where digital assets are in terms of the deployments that you are using. For example, is all of your IT and Network Infrastructure located in just the Private, Hybrid, or Public cloud, or is it segregated amongst all three or just two of them? Or if you are still using an On Premises Infrastructure, in which areas do you have your servers, workstations, and wireless devices. From here, it is important to create a high-level map as to where everything is located. This will then form the foundation as to how you will create the various Segments in your IT and Network Infrastructure. Another key advantage of using the Cloud is that you will have tools at your disposal to map this out fairly quickly.

3) Decide the authentication tools:
   If after completing the first two steps the decision is a "yes" to go with the creation of a Zero Trust Framework, then an important next step is to decide upon the kinds and types of authentication mechanisms that you and your IT Security team think will work best for the security requirements of your company. Some of the favored ones are the use of passwords, challenge/response questions, smart cards, FOBs, RSA tokens, Biometrics, etc. In fact, with some of these tools, there will be other complimentary tools that you can use as well. For example, there are other technologies that are similar to the RSA token, and you can use those in conjunction with RSA one as well. Although we have detailed the Biometric modalities of choice for a Zero Trust Framework in Chapter 3, there are still others that you can choose from, but keep in mind that they are not all commercially available yet. Another important tool that you can give serious consideration and which is widely available is known as the "SASE". This is an acronym that stands for "Secure Access Service Edge". This is a SaaS based device that creates and deploys a Virtual Machine (VM) near the devices that are requesting access to the shared resources, and processing of data. The idea is by having it closer to the end user (or employee), the transmission and transaction times will be quicker, respectively. A theoretical illustration of the SASE is illustrated below:

4) <u>Develop your Zero Trust Framework Plan</u>:
   Once you have decided on the authentication mechanisms as reviewed, the next step is to actually map as to how your Zero Trust Framework will be like, going into the granular detail as much as possible. Think of this as the security blueprint for your company. In this set of documents, you should establish every Segment in your IT and Network Infrastructure, as well as the authentication tools that will be used. There are two key things to keep in mind here:

   *This is set of documents is still theoretical in nature. So far, they have not been tested in a real-world environment. Therefore, you and your IT Security team need to literally test each and every Segment in a sandbox like environment to make sure that it is working up to expectations, and that there are no glitches which are involved. If there are any, then it must be remediated immediately. Once one Segment has been deemed to optimal, then it can be released into the production environment where your end users (or employees) will start the Multifactor Authentication (MFA) approach in order to gain access to the shared resources that they are seeking.

   *By taking the above approach, you will actually be developing the plan as to how to phase in your Zero Trust Framework. True, you and your IT Security team can test all of the Segments in the sandbox all at once, and deploy them into production that same way also, but errors are prone to happen, which could have a detrimental and cascading effect on the other layers of security. Therefore, and as also stated previously in this chapter, the Zero Trust Framework must be implemented in steps, or in phases, to minimize any kind of downtime to your business. So the bottom line here is test each component separately, then deploy it.

5) The complete deployment:
   At some point in time, after all of the diagramming, documentation, and testing, your Zero Trust Framework should be up and running in its full entirety. But keep in mind that it does not just end there. Rather, you and your IT Security team, as well as the other key stakeholders (as identified in the first step) need to keep a close eye on how things are working. If there are any issues (there will most likely be some in the first few months of actual deployment), they need to be investigated and rectified immediately before they are transmitted to the other segments of the Zero Trust Framework, if at all. Each Segment of it will be independent from this, so this risk should be minimal in terms of actual occurrence. But apart from this, your team should also be kept apprised of other new kinds of tools which emerge onto the marketplace that could potentially be used in a Zero Trust Framework. Keep in mind that you want your model to be as updated as possible in terms of newer technologies, as well as having a regular software patch/update schedule for your authentication mechanisms. In fact, if it is feasible for your organization, you may even want to consider having a dedicated Zero Trust Framework team whose primary purpose is to keep tabs with what is going on and make recommendations for improvement.

6) Always seek approval:
   As your Zero Trust Framework Model continues to evolve throughout your business, keep in mind that changes and refinements will always be made to keep up with the latest threat vectors that are appearing on the Cyber landscape. But one cannot simply change something when they want to. Rather there has to be a solid system of checks and balances in place. This is where the Change Configuration Committee comes into place. Every request for a change, or an upgrade must be brought up and approved at this level. Any action taken must also be documented, not only for the sake of compliance, but to also abide by the tenets of the various data privacy laws (such as the GDPR, CCPA, HIPAA, etc.).

Keep in mind that there are also key metrics that you can use to gauge the true effectiveness of your Zero Trust Framework Model. Some of these include the following:

1) "Mean time to detect (MTTD):

   This is a crucial element because the faster an organization identifies an attack, the greater the odds it can contain it with minimal damage.

2) Mean time to respond (MTTR):

   The ability to neutralize a threat and get systems back online is critical because as events drag out, risks and costs increase.

3) Mean time to contain (MTTC):

   This metric refers to the average time required to shut down all attack vectors across all endpoints and minimize the probability of any further damage."

The Flaws With The Traditional Zero Trust Framework Model

Up to this point in this chapter, we have reviewed the history of the basic Zero Trust Framework model, as well as the Perimeter Defense Model. As was noted earlier, many businesses are now shying away from this, as it is not a robust tool to be using anymore. Various reasons were also pointed out as well as to how the basic Zero Trust Framework can overcome the shortcomings of the Perimeter Defense model. The various aspects of the former were examined, as well as its strengths and advantages.

Finally, a set of best practices were also reviewed in detail. But believe it or not, despite the basic Zero Trusts Framework "overpowering" the Perimeter Defense model, it still has its own set of shortcomings as well. Thus, at the end of Chapter 4, we proposed our own version of the Zero Trust Framework, which we believe can overcome the weaknesses of the basic one. To summarize, here are weaknesses of it:

1) The use of MFA authentication mechanisms which can still be the target of the Cyberattacker.
2) Having to the end user (or employee) to keep verifying, and going through all of the authentication and authorization processes over and over again, each and every time they need access to shared resources.
3) No integrity checks are being conducted as authentication information and data is being transmitted to the authorization server, which grants the end user (or employee) access to the shared resources.
4) Still heavy dependence upon using the password as one of the prime mechanisms for the MFA methodology.

In the remainder of this chapter, we will address each of these shortcomings, and how our proposed Zero Trust Framework can offset these disadvantages as just described. It is important to note at this point that what we propose is still theoretical in nature, and even before it can even be launched into a production environment, ti must first be tested. Second, keep in mind that the Zero Trust Framework is designed to work in the internal environment of an organization. It is not all designed to work in the external environment.

The next section will address the first and fourth areas of weaknesses.

The Use Of Biometrics

We introduced the concept of Biometrics back in Chapter 3. Three separate modalities were examined, which are as follows:

1) Iris Recognition;
2) Fingerprint Recognition;
3) Facial Recognition.

In Chapter 4, we discussed in detail how they can be used as the primary means of both authentication and authorization in the Zero Trust Framework. The three pillars of a successful authentication are:

1) Something you are;
2) Something you have;

3) Something you know.

While this can be achieved in a real-world setting, the truth of the matter is that the second and third forms of authentication can still be easily hacked into. For example, a smart card or an even RSA token can still be intercepted. Although the smart card carries the credentials of the end user (or employee), the data packets can still be intercepted by a malicious third party using a simple network sniffer. FOBs can also be lost or stolen easily, as with RSA tokens.

With the third one, there is still heavy usage of the password, no matter how long or complex it may be. Even though a password manager can contain all of these passwords, the application can still be hacked into, because even that requires the use of a master password. In the same manner, challenge/response questions can also be tampered with, as the database which contains them can be the target of a brute force or even dictionary like attack.

So in the end, the only way an end user (or employee) can positively identify themselves is through the use of Biometrics. This is essentially where a snapshot of either the physiological and/or behavioral characteristics are captured, and the unique features extracted. So in this regard, we firmly believe that relying exclusively upon the use of Biometric technology is the way to proceed with the Zero Trust Framework. In the end, the goal is to have a passwordless environment for both authentication and authorization, and Biometrics meets the criterion for both sets of circumstances.

But keep in mind that Biometrics may not be suitable for every end user (or employee). For example, they have damage to their finger or even their iris which can be an obstacle in getting an accurate scan. Or they simply may just refuse all together to use any kind of Biometrics, as it would be a total invasion of their privacy, rights and civil liberties. So in these circumstances, a backup, or alternative method must be used.

Biometrics offers a distinct set of advantages over the traditional password, and also any smart card, or token, or FOB. These are as follows:

1) The Biometric Template is nothing but a mathematical file, which represents the image of the physiological and/or behavioral characteristics that were captured. So if for some reason, these templates were to be hijacked by a malicious third party, there is really nothing they can do about it. For example, they cannot take these files and try to use them at a Zero Trust Framework in a different organization, as each Biometric vendor has their own proprietary of processing them. In other words, stealing a Biometric Template is not the same thing as credit card theft.

2) If a Biometric Template were to be stolen, it is very easy to create a new one, in just a matter of a few minutes. There are no calls that are needed to the help desk, and best of all there are administrative costs or overhead with resetting a Biometric Template, unlike the password (where resetting them can be as much as $300-$400/year/employee.

3) Biometric Templates offer a certain degree of non-repudiation. This simply means that the end user (or employee) cannot deny that a specific template is theirs. After all, they have been enrolled by the Biometric system, and the template has been tagged with a unique identifier in the database of the Zero Trust Framework.

4) Biometric Templates can be lost or stolen. The only way that a cyberattacker can gain access to it is if they rip off the body of the end user (or employee).

5) There is little end user (or employee) training that is required. You just demo the modalities once, and that should be enough to complete all of these process:

   ➢ Enrollment;
   ➢ Verification;
   ➢ Authentication;
   ➢ Verification.

6) Biometrics offers a very high degree of accurate identification, when compared against passwords, challenge/response questions, etc.

Thus, with these compelling reasons, this is why we think that Biometric Technology should be the sole and premier authentication tools for the MFA component for the Zero Trust Framework. We also presented a sequencing model as to which modality should come first, second, and third, in order to provide the most optimal level of MFA. To summarize, it is illustrated below:
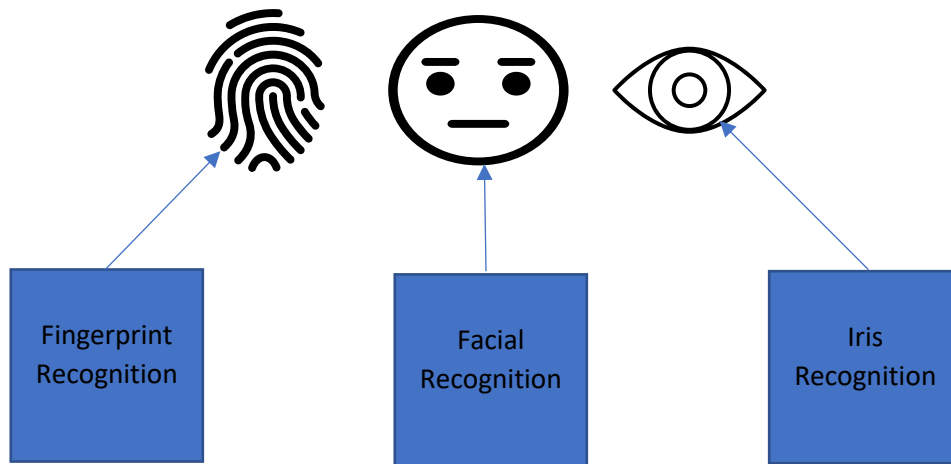
The Weaknessess Of Repeated Authorization and Authentication

The second major weakness of the traditional Zero Trust Framework is its repeated need to keep authenticating and authorizing an end user (or an employee) each and every time they need to get access to something. Although the philosophy of the ZTF is to "never trust" but keep verifying, it can really be a nuisance in the end. On top of that, having to go through this process over and over, especially for larger companies, can tax computing and processing.

But not only that, the end users (or employees) can also get frustrated with having to go through this process every single time. Is there a solution for this? Yes, and the answer resides in what is known as "Privileged Access Management. In a very broad sense, this area deals with providing a higher level of

security for those accounts that are deemed to a higher level than the regular employees. For example, this includes the likes of the CISO, network administrator, database administrator, or even the project manager on a software development team.

Essentially, anybody that has a managerial position at the IT level will have these kinds of accounts. A technical definition of Privileged Access Management (also known as "PAM") is as follows:

"In an enterprise environment, "privileged access" is a term used to designate special access or abilities above and beyond that of a standard user. Privileged access allows organizations to secure their infrastructure and applications, run business efficiently and maintain the confidentiality of sensitive data and critical infrastructure.

Privileged access can be associated with human users as well as non-human users such as applications and machine identities."

As one can see from this definition, even AI and ML can be given Privileged Level Access. It is important to note at this point that all of the authorization and authentication information and data are kept in what is known as a "Secret Vault". This is the where the automation process comes into play. For example, if a network administrator needs to gain access to a server, all he or she has to do is simply click on the application icon, and they will be automatically logged into the server.

The login credentials to this server are already stored in the Secret Vault. The network administrator will have their own Privileged Account, and the rights and privileges for the server will be stored here. So, when this individual clicks on the application icon on their desktop or wireless device, this will trigger a response to be sent from the Privileged Account to the Secret Vault, requesting that access be made to this particular server. From here, the Secret Vault will then transmit the login information to this server, and within seconds, the network administrator will be able to get into the server.

This is illustrated in the diagram below:
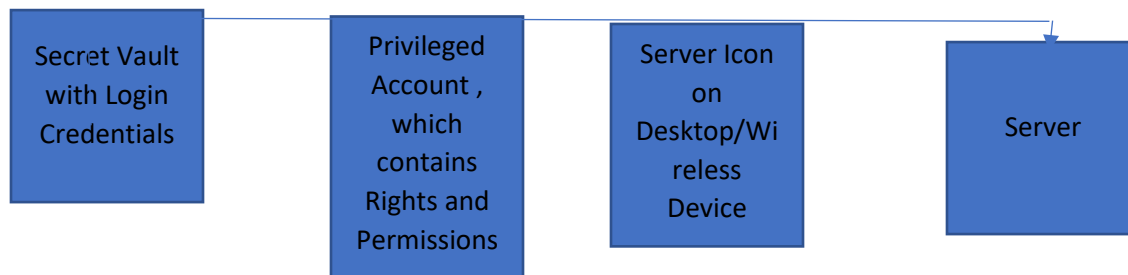
This same approach can also be used for the Biometric Templates, and this will be discussed later in this chapter. But since PAM is such an integral component of our proposed Zero Trust Framework, it is necessary to a deeper dive into it, in order to gain a much firmer understanding of it. The next few sections will get into more detail.

The Strains of On Prem PAM

Before the COVID-19 pandemic hit, mostly all businesses had an On Prem Infrastructure, or some parts of it were also located on a Cloud based platform, such as that of the AWS or Microsoft Azure. But using PAM in this manner is now showing it is not viable for the following reasons:

> ➢ The IT and Network Infrastructures of today are no longer deemed to be static in nature. Rather, they are dynamic, with many end users logging in at the same time to access shared resources, as well as the sheer influx of information that businesses have to store today in data warehouses, and the various states that they have to go through. These include if they are archived, being transmitted to different points, or are being processed and analyzed.

> ➢ Access to the above often made use of GUIs in order to access a PAM server to get the privileged login information. This was done all manually, thus adding more administrative headaches to an already strained process.

> ➢ Logging into separate applications required multiple logins into the PAM server in order to access the proper credentials. Given today's mantra for automation and APIs, and as a result, this is no longer feasible to use.

PAM based solutions are much better suited for Cloud based deployments, especially when it comes to the Hybrid Cloud, as the next section examines.

Why PAM Is Better Suited For The Cloud

As companies today make the full, 100% move to a Cloud based environment, PAM will be far better suited here for this kind of environment, foe the following reasons:

1) <u>Direct access is now a reality</u>:
   In today's world, not only do software developers want quick access to their code, but they also now have to follow the rules of DevSecOps. Having a tool such as Active Directory not only provides a secure way to give out privileged access, but the same login credentials can be used over and over again on different development tools until the so called "Time To Live" request has expired. In this case, the software developer will then have to go back to Active Directory to get a new set of privileged credentials.

2) <u>You can keep existing workflows</u>:
   It is a basic fact that humans are sheer creatures of habit. We don't want to change unless we absolutely have to. This is especially true of software developers. Once they have become accustomed to a certain way of creating source code and the tools that are used to compile it, they don't ever want to adapt to a newer way of doing things. But by using PAM in the Cloud, it allows for what is known as "Native Tooling." This allows for the software developers to keep using the tools that they have become accustomed to for so long, while adding in richer layers of authentication protocols.

3) <u>You can make use of the latest code development practices</u>:

DevSecOps not totally embraces the automation process, but it also allows PAM to support the following functionalities in the Cloud:

➢ Promote the usage of Infrastructure as a Code:

This is simply the provisioning and management of your Cloud infrastructure through the use of a certain programming language, rather than using the old fashioned, manual processes. This enhances the speed automation, and helps to cut down on the number of security related mistakes that occur in the source code creation process.

➢ Configuration as a Code:
This allows for an automated version control system to be deployed in your Cloud infrastructure. Through this, you will have increased states of visibility, automated Quality Assurance (QA) testing, and ways to revert back to older editions of the source code, if the need ever arises to do so.

4) It can help to support the various ChatOps tools:
The Remote Workforce of today is heavily reliant upon the use of various Instant Messaging (IM) tools now more than ever before. Examples of these include platforms such as Slack and Microsoft Teams. By integrating PAM here, such as Just In Time (JIT) requests allow for privileged access provisioning and approval to happen a lot quicker and more efficiently, than versus doing this on an On Premises infrastructure.

5) It will help to create a Passwordless environment:
Let's face it, the password has been the de facto standard for both authentication and authorization purposes, and while it is expected to be so, a PAM solution that has been built for the Cloud will help to totally eradicate the need for passwords. This is so because many organizations are now making their best efforts to go to a Passwordless system, such as using tokens, digital certificates, biometrics, etc.

6) It will support diverse kinds of operating environments:
Although the movement now is to have PAM support gaining access to administrative credentials that are based in the Cloud (such as that of Azure), a workable solution will also support a Hybrid like environment where credentials can be granted securely where a company makes use of a Cloud and On Prem environment. This is so because not all companies have chosen yet to make the full migration to the Cloud, some still prefer to have part of their infrastructure based on Prem.

The Advantages of Using PAM In The Cloud

Obviously, deploying a PAM based solution in the Cloud is far better than doing it On Prem. The benefits can be detailed as follows:

1) Centrally store and manage passwords:
In today's business world, passwords are amongst the biggest nemesis that is faced. For example, the cost to reset a password is pegged to be at about $100.00 per employee. If you are a smaller SMB, this may not come to a lot of money in the end. But if you are a Fortune 100

company with thousands of employees worldwide dispersed globally, this cost can add up quickly, and take a toll on the bottom line. Sure, there are other tools you can use out there, such as the basic Password Manager. But there are inherent security flaws with those as well, especially when it comes to overseeing those employees that have privileged access accounts. What makes PAM unique in this sense is that it brings to the Cloud a high powered "Password Vault" which allows to you manage and assign administrative privileges from a single dashboard, in a very safe and secure environment. Nobody else but you will be involved in this process, unless you have other IT Managers that you want to grant this kind of access to.

2) Easier to enforce the Concept of Least Privilege:
One of the cardinal rules in Cybersecurity is to give employees just enough access to shared resources for them to do their job on a daily basis. Although this sounds simple in concept, enforcing it and keeping of what employees have is another story. For example, the IT Security team may give out admin level credentials to a contractor only for the time that they are at your business. Once they are done with their work, this account should be immediately disabled, but many times it gets forgotten about. Or employees may share their passwords behind your back. Whatever the situation is, you need a tool that can oversee and execute the concept of Least Privilege on a real time basis. This is where PAM will play a crucial role. Once deployed in a Cloud environment, it can automatically assign privileges on a needed basis, following the rules and permutations that you have set forth. But best of all, it will terminate those accounts which no longer need those privileges for certain applications. In other words, you don't have to go from through every computer and wireless device to make sure that the baseline rights and permissions have been assigned and/or deleted. The PAM can store all of the employee profiles, and decide when to allocate and disable permissions automatically. This reduces the risk of forgotten accounts still being activated, which could create a potential backdoor for a Cyberattacker. This is also known as "Just In Time Access" and can even be used for members of the IT Security team in order to reduce probability of misuse of admin level privileges.

3) Control Remote Access:
With the COVID-10 pandemic still upon us to varying degrees, the Remote Workforce is here to stay permanently. While many of the initial security issues were worked out when WFH was first launched a couple of years ago, many of the traditional security tools have been stretched beyond their breaking points. A prime example of this is the Virtual Private Network (VPN). Before the pandemic hit, it did an excellent job of encrypting and securing the network lines of communications. But this was when only 15% - 20% of all employees were working from home, not the near 100% capacity we are seeing now. Thus, Cyberattacker now has greater ease in which to penetrate into the VPN, gain access to privileged credentials, and even hijack a remote session. But by implementing a PAM solution into your Cloud environment, you can make use of the Zero Trust Framework and implement what is known as the "Next Generation Firewall" which far surpasses the security thresholds that are offered by the VPN. Not only will this prevent the hijacking of privileged access credentials, but you will have logging activity recorded on a real time basis, which makes auditing far easier and simpler.

4) Protecting Interconnectedness:

92

As the digital world is coming together, so are the objects that we interact with on a daily basis, which include those in the physical and virtual worlds. This is technically known as the "Internet of Things," or the "IoT." The Cloud has also made it to a great extent these objects to interact with one another, but the problem is that the end users still have the security set to the default level, which also includes making use of a very weak password. When PAM is implemented into IoT infrastructure you have deployed into the Cloud, it can manage the creation and assignment of appropriate privileges to the end users on an automatic basis. It will even assign passwords that are far most robust than what a traditional Password Manager can create.

5) Secure DevSecOps In The Cloud:
This was a concept that was introduced in the last article. This is a merging of three distinct teams:

➢ Software development;
➢ Operations;
➢ IT Security.

One of the central themes of DevSecOps is automation. While PAM can be used here once to protect privileged access to the source code, it can even do much more than that, for example:

➢ Secure developer accounts;
➢ Secure Encryption Keys;
➢ IT Security.

One of the central themes of DevSecOps is automation. While PAM can be used here once to protect privileged access to the source code, it can even do much more than that, for example:

➢ Secure developer accounts;
➢ Secure Encryption Keys;
➢ Secure Digital Certificates.

A Best Practices Guide for Deploying a PAM based Solution.

Just deploying the Zero Trust Framework, deploying a PAM based solution takes careful planning, and testing before releasing it into the Production Environment. Here are a few tips to help ensure a smoother deployment:

1) Understand why you need PAM in the first place:
You simply should not deploy a PAM solution just because you think you need to. You first need to think carefully why you need one in the first place, and if you decide to have one, then you need to map it very carefully how it will fit into your IT and Network Infrastructure. You need to fully ascertain which systems, processes, and technologies will be requiring this. Then you need to figure out who will have access to the PAM solution these are keys to the proverbial crown jewels of your organization.

2) Create a PAM password policy:
You should already have a password policy in place, but the one for PAM will be different in the sense that you need to craft it so that it addresses the needs of those that have managerial or IT

admin titles. Having such a policy in place will help to avoid any misuse of credentials, as Cyberattackers love to go after these kinds of passwords. Therefore, it is recommended that you follow the guidelines from entities as SANS, NIST, and ISO. Remember to change out passwords on a regular basis, and just like for your regular employees, they should be made long and complex and just a little bit more, as these credentials will give access to the most sensitive areas of your business. Also, make sure you implement Multifactor Authentication (MFA) to make sure 100% that only the legitimate employees have access to privileged accounts. Some of these second and third layers of authentication can include the use of passphrases, RSA tokens, Smart Cards, Biometrics, etc.

3) Change out default passwords:
   Once you have created a privileged account, make sure that the person to whom it is assigned immediately changes the password. Even though the default password may be long and complex, it is always a good practice to make sure it is changed out when the account it is first activated. Make sure you put into your PAM security policy as to what these passwords need to contain. This will be an alphanumeric string, but to what detail it needs to contain needs to be spelled out to avoid any confusion or mistakes. Remember, your employees do not have to create these kinds of passwords. The PAM functionality should take care of all of this on an automatic basis. But it is always a clever idea to conduct an audit from time to time as to who has what access when it comes to privileged accounts.

4) Keep tabs as to what is going on:
   Just as much as the IT Security team has their eye on the Cyber Threat landscape, you also need to keep an eye as to what is happening to the privileged accounts that you assigned. For example, you need to make sure that those employees who have these kinds of accounts are abiding by every letter of the PAM password policy. Of course, you will not be able to keep track of all of this on a 24 X 7 X 365 basis, so this is where you can use the tools of both Artificial Intelligence (AI) and Machine Learning (ML). They can keep an eye for you on these accounts on a real time basis, and alert you in case there is any type of anomalous or suspicious behavior that is transpiring. Keeping track of all this will give you the essential metrics that other members of the C-Suite will ask for, and even the Board of Directors. Keeping track of this will also be very advantageous to you in case you are ever faced with an audit by regulators from the GDPR, CCPA, HIPAA, etc.

5) Make use of Least Privilege:
   This was reviewed in one of the previous articles. With this, you are assigning the minimal amount of permissions that are necessary for your employees to conduct their daily job tasks. But this holds true also for those employees that have privileged accounts. Just because they are technically at a higher plane because of the level access, you still need to follow the concept pf Least Privilege here as well. For instance, you would grant your IT Security Manager access to all of the devices in your company, so that they can install the needed software patches and upgrades, and perform other troubleshooting tasks. For your Network Administrator, you would assign those rights and permissions that are needed to gain access to the network, the servers, etc. These are privileges that your IT Security Manager would not need, and vice versa.

6) Deletion of temporary accounts:

94

At times, it may be necessary for you to set up a privileged account for an outside third party, especially if you hire a vCISO. Rather than assigning an original, privileged account for them, create a cloned account, and from there, you can then specifically configure the privileged access this individual will need, based upon their contractual obligations to you. Set this account to be inactive on their last day. This way, you will not have to worry about forgetting about this task, it will be done automatically for you.

The Mistakes That Are Made When Deploying PAM Solutions & How To Fix Them

Even despite the care that you and your IT Security take, mistakes are always inevitable. Here is the common list of mistakes made and how to correct them:

1) How up to date are your systems?
   The PAM solutions of today are mostly compatible with the latest technologies. For example, deploying a solution for Windows 10 will not work for Windows 8, as it is a much more out of date system. Before you deploy a PAM configuration, it is very important to make sure that it will work with all of the digital assets in your business. The best way to do this is to take an inventory of all of the hard wired and wireless devices that you have. If anything is outdated, then it is time to discard and upgrade ASAP. This is not just from the standpoint of launching PAM, but it is a rule of thumb in Cybersecurity that any outdated device can pose a serious risk, as this is one of the first items that the Cyberattacker will go after.

2) Not applying passwords properly:
   This has been a widespread problem for decades, and it is only getting worse. Many employees are given admin passwords, whether it is intentional or not. By doing this, they will be able to login into the most sensitive areas of your business, and cause any type of havoc, such as data leakage. Or worst yet, they can accidentally give out these passwords to a Cyberattacker in a Social Engineering attack. Password sharing still remains a huge problem as well, and this is one of the leading causes for Insider Attacks to precipitate. To avoid all of these problems, you need to separate out the normal, everyday employees from those that are eligible to have privileged access. The former group should have its own set of security policies, whereas the latter should have its own as well. While both should be enforced equally, the group of employees with privileged access needs to have further scrutinization. In other words, you don't want to have password misuse here, as the effects can be far more serious. You are dealing with privileged accounts. In order to make sure that all is airtight, it is imperative that you check for any types of suspicious behavior on these types of accounts. This can include multiple login attempts that have failed, or trying to login to a resource to which they have no business in doing so. You can keep a daily watch on all of this by implementing AI tools, and having any alerts or warnings transmitted to the SIEM, where a dedicated member of the IT Security team can proactively tirage them.

3) Create the right kinds of profiles in Active Directory:
   One of the primary benefits of AD is that you can create as many user groups as you need, and from there, assign privileges on ad hoc basis. For example, you can create a user group for all of the accountants that work in your company, and import into that all of the individual

usernames. From there, you can create all of the privileges for that profile, and deploy all of the privileges and permissions in a simultaneous fashion. While this is certainly advantageous, it can also prove to be a serious mistake from the standpoint of the privileged user groups. You do not want a help desk specialist to have network administration privileges assigned to them by accident. So in this manner, you are probably better off assigning rights and privileges to privileged accounts manually, rather than on ad hoc basis. True, this will take more time, but at least you will have confidence that the appropriate permissions have been applied. This is where having a separate list created for the privileged accounts will be very useful, as described earlier in this article.

4) <u>The move to the Cloud</u>:
The movement to the Cloud is now happening at a pace than it was ever imagined. A lot of this has been fueled by the COVID-19 pandemic, and in this rush, security is now a forgotten topic here. When you move all of your applications to the Cloud, you need to take an inventory of what you have just moved, and from there, determine which of those assets need the highest level of protection. Of course, you will need some sort of PAM architecture here, but this too will need to protect as well. In other words, you simply cannot assign privileged accounts and merely trust your IT Security team will not run off with them. There could be a malicious threat actor here as well. Therefore, you will even need to keep a careful eye here, because in today's world, you simply cannot trust anybody anymore, even those employees that have been around for a long time. In other words, the days of having implicit trust even in the most minute degree is now over, it is time for the Zero Trust Framework.

5) <u>Outside vendors</u>:
As the world becomes more interconnected partly fueled by the Internet of Things (IoT) revolution, businesses are becoming more dependent now upon hiring third party contractors to help meet customer demands and expectations. It is highly recommended these days that you have a deep vetting process in place before you make a selection. But this is where most companies make their mistake. They don't continually monitor the hired third party after the fact. It is very important that you do audits on a regular basis, in order to confirm that there are no leakages of your datasets, and that all privileged accounts that have been assigned are not being misused in any way.

The Importance Of Just In Time (JIT) Access

In the world of supply chain management, there is a concept known as "Just In Time Inventory". This is when the raw inputs are delivered to the manufacturer right before they are needed to complete the final product. The idea here is to eliminate excess inventory in an effort to cut unnecessary costs. This is also somewhat similar to JIT Access, but instead, it deals with the establishment of the rights, privileges, and permissions that are needed in a privileged account, and is assigned to a specific role right when it is needed the most.

To illustrate this example, take the role of the Project Manager that is overseeing a software development team. This group is developing a web-based application for a client, and the Project

Manager needs to gain superuser network access in order to see how the prototype product will work on both the front and back ends of a server.

To accomplish this, the IT Security team will provide JIT Access that is designed specifically for the role of a Network Administrator. During this time, the Project Manager will then see how the protype runs, and make any notes of tweaks and adjustments that need to be made to the source code. Once this task is over, the IT Security team will then completely disable the JIT Access until it is needed again for a similar situation.

This example illustrates what JIT Access is, and from the standpoint of a specific role. In a company, there can be accounts that are established for specific privileged roles, with all of the rights and permissions that go with them. So when is absolutely needed, it can be activated, and once the work is done, it can be disabled, or deactivated once again.

The basic idea of JIT Access is to avoid keeping privileged access accounts in an always "on mode", which can be a huge risk from the standpoint of Cybersecurity. It is also based upon the principle of "Least Privilege", which states that only the minimal rights and permissions should be given, even in the case of super user accounts, like PAM.

<div align="center">The Types Of JIT Access Accounts</div>

There are a number of role-based JIT accounts that can be created, and some of them are as follows:

1) Justification based Access:
   This can also be referred to technically as the "broker and remove" accounts. For example, if the Project Manager needs to have Network Admin privileges, they have to provide written justification to the manager of the IT Security team why this kind of access is needed and for how long. Once this is deemed to be satisfactory enough, the Project Manager is then given this type of role-based access once it is needed, and will terminate immediately once the work is done. The written justification must also include the tasks that will be done, and anything that is done outside of these bounds will red flagged as suspicious behavior, and thus, the Project Manager will be stripped of this super user access immediately. It is important to note here that the login credentials of these JIT Accounts are locked in a separate vault, and remains unknown to most people in the organization.

2) Ephemeral Accounts:
   In this situation, JIT access is given to complete just one specific task. For example, if you bring in a third-party contractor to deploy a certain piece of software en masse to your employees wireless device, then you will be giving them only this kind of access. Once the work is done, this account will then be deleted by the IT Security team.

3) Privilege Escalation:
   This kind of JIT Access is used for your longer time employees, typically the direct hire ones. Going back once again to the example of the Project Manager, if he or she needs only a subset of the Network Administrator rights and privileges to complete just a few tasks, then you can add these permissions into their existing PAM account. Then once the Project Manager is done completing their tasks, these elevated permissions can then be quickly removed from their

existing PAM account. One of the advantages to this is that there is no need to waste time switching complete accounts over, and flipping them back later, which can cause a security risk.

The Benefits Of JIT Access

There are numerous strategic advantages to using this kind of approach, some of which are as follows:

1) The level of Cybersecurity is improved:
   When employees are given just what they need to access shared resources at the most minimal level possible, your Cybersecurity posture will be greatly strengthened. There are no lingering privileged accounts out there that the Cyberattacker can take advantage of, and by taking this kind of approach, your attack surface also decreases.

2) The assignment of accounts can be automated:
   JIT Access can be provisioned on an automatic basis, thus eliminating paperwork and the time it takes to grant formal approval.

3) It can be applied to other areas:
   JIT Access can be flexible as well, and it is not a rigid methodology. For example, software developers can be given JIT Access in order module templates which supports the workflows of the DevOps team. This is crucial when it comes time to creating software builds and QA testing them. The concept of JIT Access can be applied to other departments in your organization as well. For example, if the Finance team needs to have access to employee salaries, JIT Access can be used so that they can retrieve this data from the Human Resources department for the time period that is needed.

4) Easier management of third parties:
   Whenever an outside contractor is hired, there is always some fear that they might be given more access than what is needed. But by using JIT Access, this problem is negligible, especially if you are using Ephemeral based accounts.

The 4 Pillars To PAM Success

The top four major components that the CISO and his or her IT Security team need to examine are as follows:

1) Track every account:
   A privileged account is one which has some super user privileges to a certain degree. These credentials could involve things such as database administration, network administration, security administration, etc. Therefore, these kinds of accounts need to be safeguarded very carefully, and constantly monitored. After all, if a Cyberattacker can gain access to just one on Privileged Account, then the chances are much greater that they will be able to move laterally in a quick manner to your digital assets. Therefore, any good PAM solution should have functionality to keep track of each and every account that has been, even if it is for just a few hours. Also, the solution must be capable of either deleting or deprovision any inactive PAM

based accounts. Also, information about the use of Privileged Accounts needs to be collected which will form your governance strategy as to how they will be given out in the future.

2) <u>The limiting of access control</u>:
There are two characteristics of Privileged Accounts that you need to be aware of: 1) Access Control; and 2) Access Governance. With the former, you need to keep track of all of the changes that are made in the Privileged Accounts itself. For example, these accounts can be regarded to be dynamic in nature. The profiles and the groups in these accounts will change over time, depending largely on how the security policy of your organization changes. Thus, the IT Security team must keep track of these changes. If there are too many of them being made from the established baseline, then this could be a cause for concern. With the latter, you need to keep track of what Privileged Accounts can access what. You do not want any crossover between the entitlements that have been established for a network administrator to have database privileges. In other words, a Privileged Account should only give access to what is urgently needed for just a brief period of time.

3) <u>Record activity</u>:
Any good PAM based solution must give the CISO and the IT Security team the ability to capture the activity of all of the Privileged Accounts on a real time basis. The reason for this is that this data will prove extremely valuable when it comes down to doing an internal audit, or even one that may be conducted by federal regulators. However, parsing through all of this data can be a very burdensome task, and can even prove to be an administrative nightmare. Thus, the PAM based solution must have the ability to give a visual representation to all of the information that is being collected. Moreover, it should also have the functionality for the IT Security team to build specific queries not only to extract data, but to also examine what if scenarios down the road.

4) <u>Automation</u>:
In today's world, the IT Security team is inundated by threat vectors on a minute-by-minute basis. Although Privileged Accounts is constantly a high a priority, it cannot be done by a human being; it is just too much to ask for. Therefore, any PAM based solution must have automation built into for the following, to just name a few:

*Doing mundane and repeatable tasks;

*Establishing configuration changes;

*Conducting software upgrades and patch maintenance;

*Service shutdowns and startups;

*Event log management;

*The establishment of Multifactor Authentication.

The Finer Points of Privileged Access Management

As you deploy the Zero Trust Framework for your organization, keep these granular details in mind as well:

1) Privileged Access Governance:
   We all know that most organizations have higher level accounts than from the rest of the employee base. These are the Privileged Accounts, and these are typically assigned to those employees that have some sort of administrative role, such as a network or even a database manager. Even a project manager on a web development project could very well be assigned a privileged account so they can oversee the project from beginning to end. Although the goal of a PAM based solution is to properly govern these accounts when they are needed and not needed, they do not observe how the privileged end user actually interacts with the sensitive data to which they have been access to. For example, are there any malicious activities that are transpiring? Are these privileged accounts being abused in any way. This is where the Privileged Access Governance component comes into play. From this, in a single view, you can see any signs of abnormal behavior towards the data. There are log files that are provided for this very reason, so you will be able to get any first indicators of an insider attack that could be brewing. This comes all under the umbrella of what is known as "User Behavior Analysis". The Privileged Access Governance functionality can also draw out various visual diagrams as to where all of your sensitive datasets reside at. This is especially useful to have in order to come into compliance with various data privacy laws.

2) PAM Discovery:
   If the organization is especially large (starting at a 1,000-employee size or greater), Privileged Accounts can be created and used without even the IT Security team knowing about it. The primary reason for this is that it is the job of the IT department to do all of this. Very often, there is a lack of communication between both parties, and quite often, one party does know what the other is doing (and vice versa). Therefore, you need some sort of functionality in your PAM based solution to keep of any Privileged Accounts that are being created and onboarded. This is where the PAM Discovery component will come into use. Scans can be triggered automatically and messages sent to the IT Security team whenever a brand-new Privileged Account has been initiated and onboarded. This functionality will also give you the ability to keep a continuous eye on those Privileged Accounts and recycle those that are outdated into a newer state with updated rights, privileges, and permissions.

3) Privileged Credential Management:
   This can also be referred to as "Privileged Password Management". However, this is not to be confused with that of a Password Manager. This refers to just the creation and storage of passwords for the everyday consumer, who has many passwords to remember. The Privileged Credential Management component of a PAM based solution keeps track of those login credentials that are strictly associated with Privileged Accounts. Technically, it can be specifically defined as follows:

"It is the secure storing, sharing, creating, and handling of privileged passwords. Privileged password management may alternatively be referred to as privileged credential management, enterprise password management, enterprise password management, enterprise password security. Privileged passwords are a subset of credentials that provide elevated access and permissions across accounts, applications, and systems."

(SOURCE: https://www.beyondtrust.com/resources/glossary/privileged-password-management)

As can be seen from the definition above, privileged passwords are just one part of all of the passwords that are established for all of the other employees of a company. But it is considered to be a subset, given the special characteristics that they have. But passwords are only set of credentials that can be used with PAM based solutions. These include tokens, SSH keys, etc.
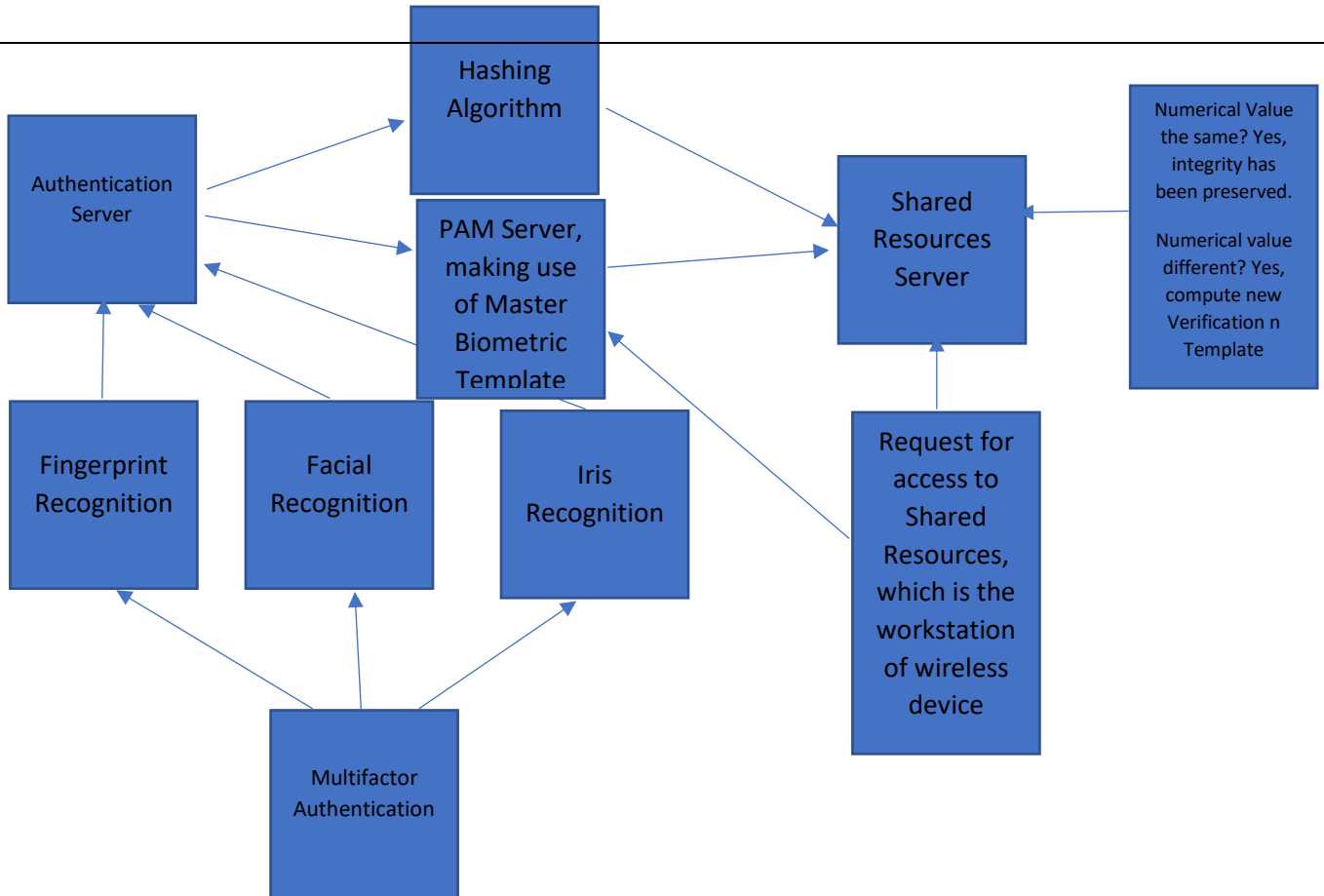
Because of the sensitivity that is involved with credentials associated with PAM accounts, they have to be monitored in a much different way than other password management techniques. In this regard, some of the best practices include the following:

*Keeping a constant eye on these kinds of credentials;

*On a 110% level, privileged credentials must be rotated on a regular basis per the security policies that have been established;

*Bring all of the privileged credentials into one central location, which is known as the "Vault";

*Keep an on malicious behavior that can impact any PAM based credential. This should be an automated basis, which will most likely make use of AI and ML plug ins to comb through all of the log files.

Privileged Session Management:

This component of a PAM based solution is meant to serve as a system of checks and balances. For example, if a network administrator logs in using a Privileged Account, then he or she can be observed on a real time basis by the IT Security team from the moment they log in, when they are in session, and when they log out. The primary objective here is that somebody else with the same privileges can keep an audit trail by another person who also has the same types and kinds of privileges. This can also serve to be very advantageous for compliance reasons.

In Chapter 4, we presented an initial model of our proposed Zero Trust Framework model, towards the end. In this chapter, we have broken down that model, and discussed thus far, how it can overcome three of the weaknesses of the basic Zero Trust Framework model. So, it is now important to review how the concepts of Privileged Access Management (PAM) will fit into our proposed model. This is what we have so far:

Hashing Algorithm

Authentication Server

PAM Server, making use of Master Biometric Template

Shared Resources Server

Numerical Value the same? Yes, integrity has been preserved.

Numerical value different? Yes, compute new Verification n Template

Fingerprint Recognition

Facial Recognition

Iris Recognition

Request for access to Shared Resources, which is the workstation of wireless device

Multifactor Authentication

To summarize the key steps:

1) The end user (or the employee) requests access to the shared resources, by clicking on the appropriate icon.
2) This then transmits a message to the PAM Server, which then pings the Authentication Server to send over the Master Biometric Template to the Shared Resources Server. Note that in Chapter 4 that this was referred to as the "New Verification Template", which is a combination of the Fingerprint, Facial, and Iris Recognition Templates.
3) Authentication to the Shared Resources Server happens in just a few seconds.

Thus, as one can see from the diagram above, repeated authentication and authorization are no longer needed in our proposed Zero Trust Model.

The next thing you will notice is the use of Hashing Algorithms. This is to ensure that the Master Biometric Template remains intact on the route from the Authentication Server to the Shared Resources Server. But even here, Hashing Algorithms are prone to Cyberattacks as well, and will be addressed in the next section. Also, this model as depicted will be updated in the next section as well, which will present the final one. In it, we discuss how Quantum Mechanics, BioCryptography, Public Key Infrastructure and various other mechanisms will come into play.

The Use Of Quantum Mechanics In Our Proposed Model Of The Zero Trust Framework

We have now approached this phase of the book where we discuss how the concepts of Quantum Mechanics could possibly fit into our proposed Zero Trust Model. But has it has been mentioned before, Quantum Mechanics is still very much a theoretical field in the work of physics, so we propose in this part of chapter is strictly theoretical. But we do believe that as research and technology continue to evolve over time, it could become a reality one day.

But before delving any further, is first important to provide a definition of what Quantum Mechanics is all about. Technically, it is defined as follows:

"Quantum Mechanics is the study of very small things. More specifically, it's the study of how matter and energy interact on the scale of atomic and subatomic particles."

(SOURCE: https://revolutionized.com/quantum-mechanics-101/)

In a small way, it can be likened to that of the Internet of Things (IoT). In this instance, there is the study of how things interact with each other in both the physical worlds. But the difference here is that we can actually see and even hold some of these objects in our very own hands. But with Quantum Mechanics, these objects are at the atomic and/or the subatomic level. This area has a number of key properties that are associated with it, and they are as follows:

1) Positioning:
   The position and the motion of a particle are mathematically indeterminate. But if for some reason you can figure out the momentum, it will be that much more difficult to compute the location of it.

2) Quantization:
   Objects in the world of Quantum Mechanics have only discrete, mathematical values that are associated with it. If any of the characteristics of these objects change, they do not do so in a gradual manner. The values with them change in a "hard" manner, without taking a slower, more measured approach.

3) Tiny Particles:
   Matter is composed of electrons, protons, and neutrons. It is also composed of light, and the particles that are associated with that are known as "Photons", which will be reviewed later.

4) Quantum Entanglement:
   This is concept where it demonstrates what is known as "nonlocality". It means that the particles are on a mathematical level, permanently correlated with one another. Although these particles are quite far apart from one another, any effect on one will have an immediate effect on the   remaining particles.

Finally, there is an area of Quantum Mechanics that is fast emerging beyond the realms of just theory. It is known as "Quantum Computing". This makes use of uncertainty and the latest principles of data science to come up with a newer and faster way to store what is known as "Bog Data". These datasets are broken into "Quantum Bits", or "Qubits", and are considered to be either in of two states: on or off.

Quantum Cryptography

A subset field fo Quantum Mechanics is what is known as "Quantum Cryptography". As you can see, Cryptography plays a huge part in our proposed Zero Trust Framework model. But a specific area of this is known as the "Quantum Key Distribution". A technical definition of it as follows:

"The process of using quantum communication to establish a shared key between two trusted parties so that an untrusted eavesdropper cannot learn anything about that key."

(SOURCE: https://sectigo.com/resource-library/quantum-cryptography).

In the model that we proposed at the very end of Chapter 4, there was an illustration of the Key Distribution Center (also known as the "KDC"). This acts as a tool in which digital certificates (which are also known as the public and private keys) could be created and issued in an efficient manner to both the Authentication Server and the Shared Resources Server. In fact, there was even a review of it as well. But despite all of the safeguards that have been taken to help protect it, it can still be prone to a Cyberattack.

Therefore, we will pay very close attention to the KDC in this part of the Chapter. So far, we have corrected three of the four major weaknesses of the basic Zero Trust Framework, which are as follows:

1) Using Biometric Technology as the sole means for MFA;
2) Getting rid of the repeated need for verification;
3) Eliminating the need for the password in its entirety (again, by making use of Biometric Technology).

There is one more flaw that still remains, and that is providing a more robust way for the integrity checks of the Master Biometric Template, as it is transmitted from the Authentication Server to the Shared Resources Server. We have pointed out in Chapter 4 that Hashing Algorithms can be used, but they have their own security flaws as well (this is where the use of Photons would come into play.

So in the end, there are three parts left before our proposed Zero Trust Framework Model can be considered to be complete, at least on a theoretical basis:

1) Adding further levels of protection to the Public Key Infrastructure;
2) Using the Quantum Key Distribution Center;
3) Making use of the Photon Particle Structures.

Once all of this has been reviewed, we will then provide an illustration of all of this. But before we go into any further detail, we believe that a formal Review of the Literature of what we are proposing should also be included.

This is the topic of the next section.

The Literature Review

One of the more powerful and recent research studies of the Quantum Key Distribution Center was conducted by Ram Kumar Jayaraman and Manoj Kumar. Their work was entitled "Quantum Cryptography and Quantum Key Distribution".

The basis for their theoretical work states that the digital certificates (the Public Key and the Private Key) are distributed between two endpoints (in our proposed model of the Zero Trust Framework, this would be the Authentication Server and the Shared Resources Server) using a series of photon-based particles. There are four major components here for Quantum Key Distribution, and they are as follows."

1) The Heisenberg Uncertainty Principle:
   A scientist, known as W. Heisenberg, ran a series of experiments in order to accurately gauge the mathematical position of any electron, by making use of a gamma ray microscope. While the location of electrons can be accurately determined, the others cannot be measured, because it

would disrupt the entire quantum-based system. As it relates to our proposed Zero Trust Framework, a private key can be sent from the Authentication Server to the Shared Resources Server and can be done by making use of a single photon. The advantage here is that a Cyberattacker can maliciously intercept a photon in transit without disturbing the integrity of the states of the other photons. Thus, this provides another unique to positively identify the specific threat variant which has been launched.

2) The Quantum Entanglement:
This is where a single photon can be split off into two separate ones, by making use of a laser beam. This causes the two photons to be entangled from within each other, and while the property of one photon could potentially be measured, the other cannot be quantitatively determined. This could be another advantageous way to protect the integrity of the Master Biometric Template. In other words, while it could be possible for a Cyberattacker to intercept one photon, there is nothing that they can do to the other photon, as its location will not be known. This is illustrated in the diagram below:

Particle A, in an Upspin

Particle B, In a Downspin
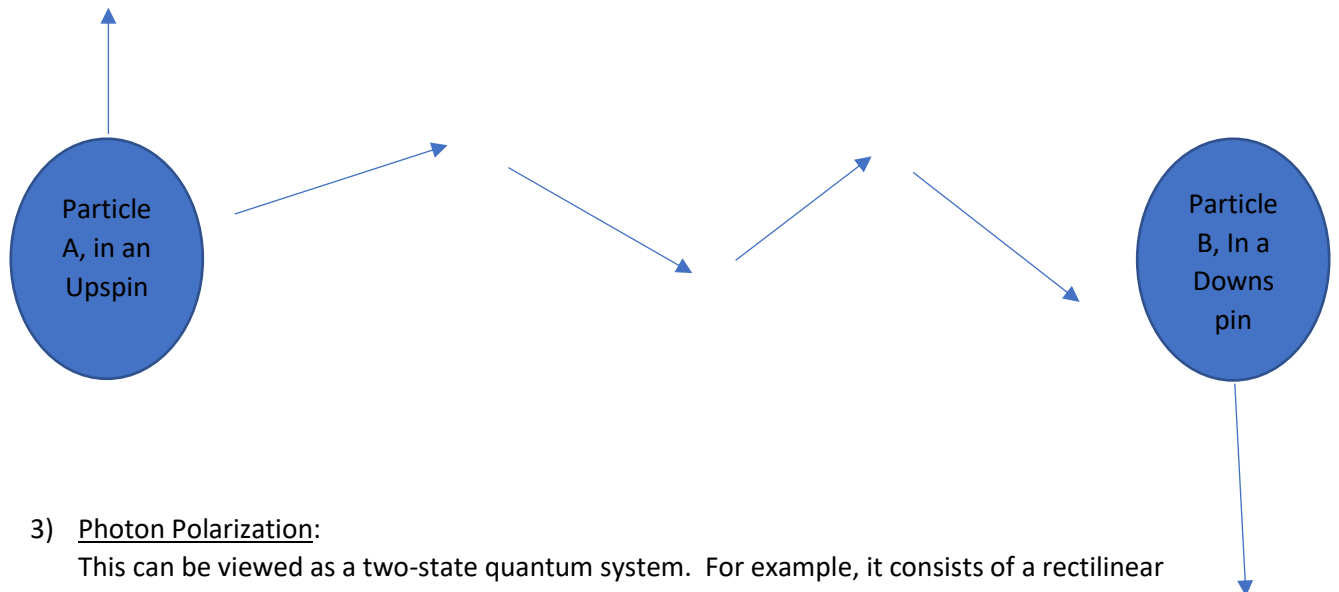
3) Photon Polarization:
This can be viewed as a two-state quantum system. For example, it consists of a rectilinear polarization basis and a diagonal polarization basis. With the former, the structure of the photons can be represented with either a 0-degree (horizontal) or 90-degree (vertical) quantum state. With the latter, it can be represented with 45 degree or 135-degree direction. The polarization of a photon is known only at the time of actual measurement. It plays a major role in preventing integrity issues in communications, where eavesdropping attacks are common. This is illustrated in the diagram below:
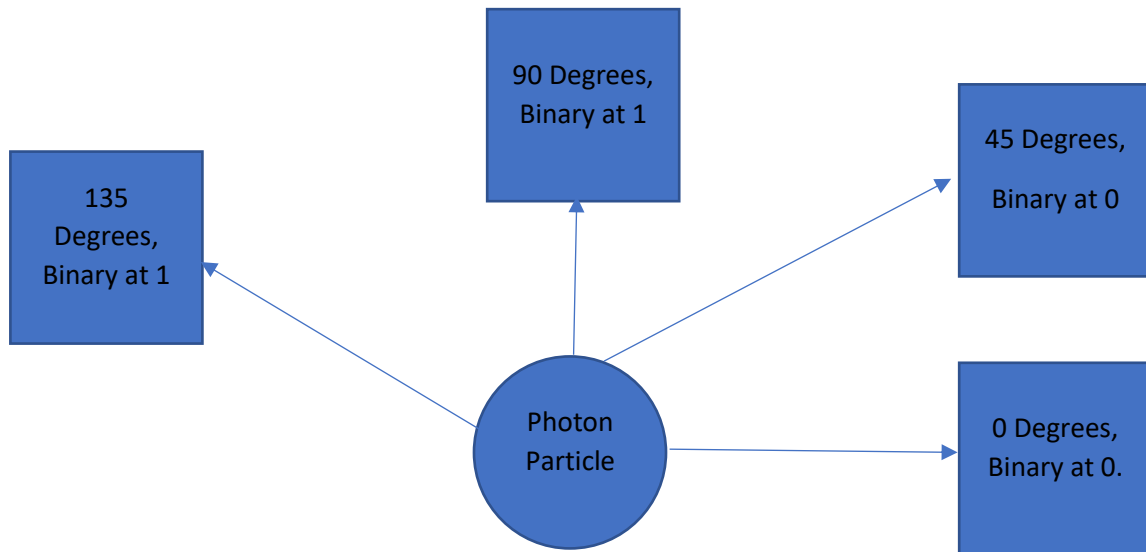
4) Quantum No-Cloning:

This is where an unknown quantum state cannot be cloned, thus it is called a "No-Cloning Theorem". In this kind of instance, a Cyberattacker cannot modify the information and data that is being transmitted between a sender and a receiver, in other words, there is no further amplification that is involved.

5) The Ekert's Protocol:

This is where the concept of photon entanglement comes into play. is used here. The photon's source is created by either the sender (the Authentication Server) or the receiver (the Shared Resources Sever). The source transmits entangled pairs of photons. The photons are entangled because the directions in which they are spinning are not known. This is yet another effective way to ensure the integrity of the Master Biometric Template as it makes its way across the two servers. This is illustrated in the diagram below:
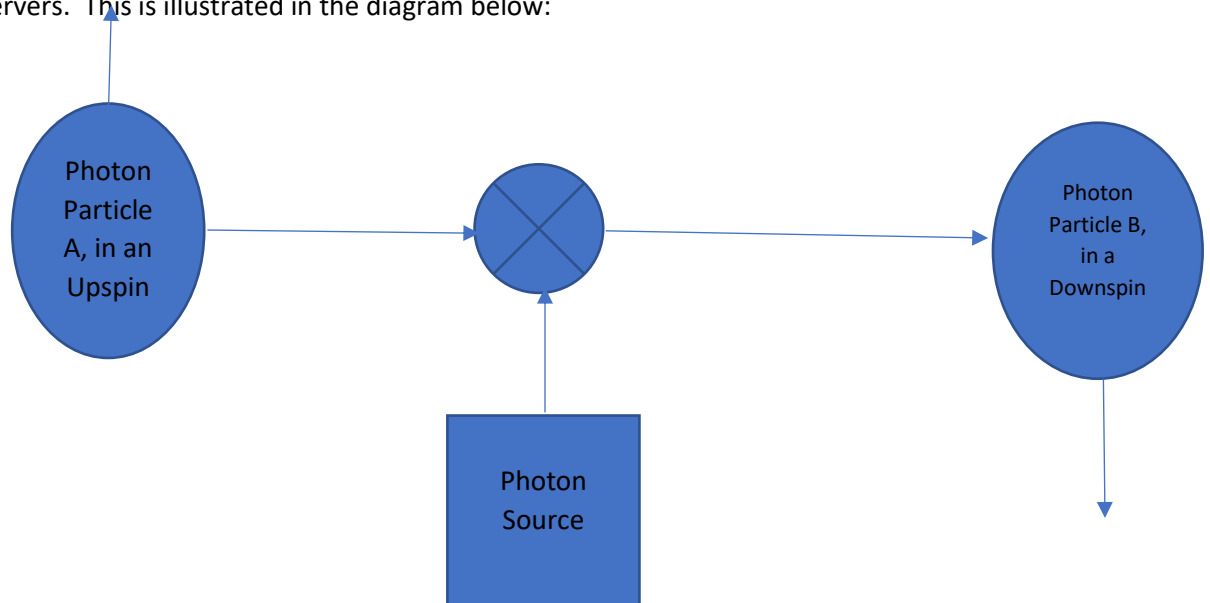
The Quantum Key Distribution Center (QKDC)

In our proposed Zero Trust Framework Model, the QKDC will establish a shared private session between the Authentication Server and the Shared Resources Server by making use of a series of photons to transmit Master Biometric Template over the optical fiber cable. This is all based upon the Heisenberg uncertainty principle, as described previously in this chapter. In summary, it states that namely, that photons are generated randomly in one of two polarized quantum states. Further, the property of a photon cannot be computed without altering the information in the photon itself.

As long as the photons remain in an unaltered state, then the integrity of the Master Biometric Template can be assured. But, if there is a change in state of even a single photon in the array structure, then the Authentication Server and Shared Resources Server will know that the Master Biometric Template has been compromised and cannot be trusted.

It is important to keep in mind at this point that the QKDC can support three types of certificates, which are as follows, and they all still live up to the standards of the X.509 protocol:

1) <u>Quantum Safe Certificates</u>:
   These make use of quantum encryption algorithms, pending approval by the National Institute of Standards and Technology (NIST).

2) <u>Hybrid Certificates</u>:
   These kinds of certificates contain a traditional RSA key and signature, as well as quantum-based key and signature. This type of certificate will be for an organization to get prepared for a full migration to a Zero Trust Framework that makes use of Quantum Mechanics.

3) <u>Composite Quantum - Safe Certificates</u>:

   These kinds of certificates are close to Hybrid Certificates because they contain a series of keys and signatures, but are different in the sense that they use a combination of existing and quantum-safe encryption algorithms.

As it was stated numerous times throughout this book, you simply cannot migrate to a Zero Trust Framework in fell swoop, especially if it makes use of the concepts of Quantum Mechanics. It is always best to use a phased in approach, and here are some guidelines in doing that:

➢ Make sure that the Public Key Infrastructure (PKI) you are using can support the QKDC. Most PKIs of today have some sort of key infrastructure, but they must support quantum certificates.

➢ The Authentication and the Shared Resources Server must also be updated in order to support both quantum-based certificates and the photon particle array structures.

➢ Confirm that the applications which are stored in the Shared Resources Server are updated so that they can also support the use of quantum certificates and photon particle array structures.

➢ Every PKI has what is known as a "Root Store". This contains all of the digital certificates that are considered to be at the root level. But, when making the move to a Zero Trust Framework based on Quantum Mechanics, this Root Store has to be upgraded as well so that it can handle the quantum-based certificates.

➢ Make sure to get rid of all of the old digital certificates, especially the RSA based ones.

The Photon Particle Array Structures

As it was reviewed in Chapter 4, it is the Hashing Algorithm that is primarily used in PKIs today in order to confirm the integrity of a message that was sent from the point of origin to the point of destination, and vice versa. Essentially, by using this kind of technique, a numerical value called a "Hash" is computed. If this number stays the same from Point A to Point B (and also vice versa) then one can confirm that integrity of the message has been intact, and it has not been altered in any way in transit.
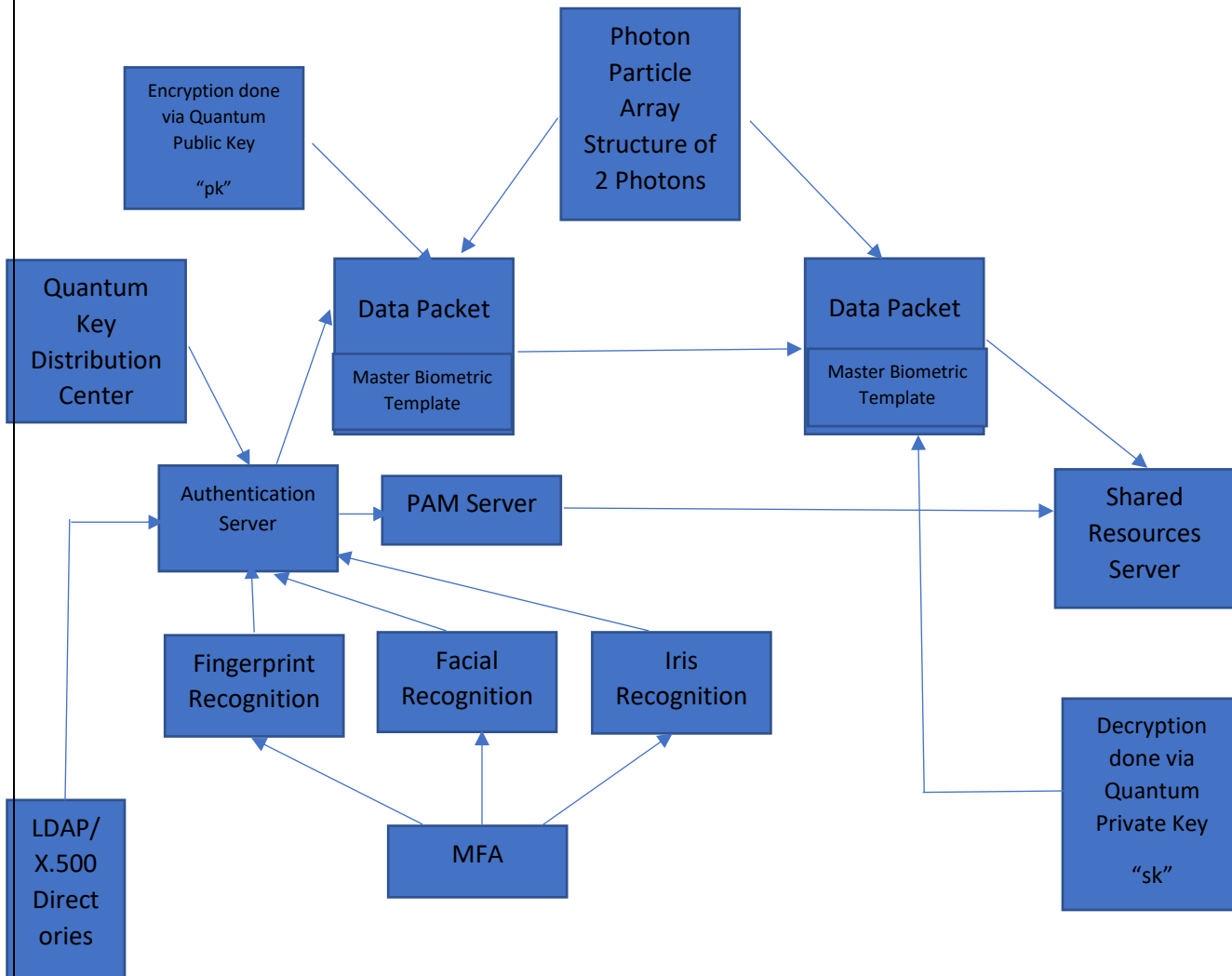
But the Hashing Algorithm is prone to Cyberattacks as well, therefore, in our proposed Zero Trust Framework, we make use of the Photon Particles as a replacement for the Hashing Algorithm. In this regard, we propose an Array Structure of at least two Photon Particles. This can be constructed by using any of the theoretical frameworks discussed earlier in this chapter. For example:

1) With the Heisenberg Uncertainty Principle:
   If one Photon Particle is hijacked by the Cyberattacker, the integrity of the other will still remain intact.

2) With the Quantum Entanglement:
   If one Photon Particle is maliciously captured, the location of the other will be indeterminate.

3) With Photon Polarization:
   The vector orientations of both Photon Particles will remain unknown, thus making this one of the strongest options to use.

4) With Quantum No – Cloning:
   Under this scenario, both Photon Particles cannot be cloned, making this a very secure option as well.

5) With the Eckert's Protocol:
   In this scenario, the two Photon Particles are spinning in an unknown rotation, which can be very difficult for the Cyberattacker to accurately quantify. This is also yet another strong and viable option to use.

The primary reason for choosing a two Photon Particle Array Structure is that if one Photon were to be maliciously intercepted, the second will act as a form of redundancy, thus ensuring the continued integrity of the Master Biometric Template.

Our Proposed Zero Trust Framework Model

Finally, taking into account the updates made to remediate the flaws of the Basic Zero Trust Framework Model, our model now looks like this:

```
Encryption done              Photon
via Quantum                  Particle
Public Key                   Array
                             Structure of
"pk"                         2 Photons

Quantum
Key              Data Packet              Data Packet
Distribution
Center           Master Biometric         Master Biometric
                 Template                 Template

          Authentication    PAM Server                        Shared
          Server                                              Resources
                                                              Server

      Fingerprint     Facial        Iris
      Recognition     Recognition   Recognition
                                                   Decryption
LDAP/                                              done via
X.500                    MFA                       Quantum
Direct                                             Private Key
ories
                                                   "sk"
```

Here is a detailed description of how our proposed Zero Trust Framework Model works:

1) The end user (or employee) first gets enrolled into the Authentication Server by completing the Enrollment Process. This means going through each of the Biometric Modalities as depicted above. At this stage, the Enrollment Template is created, and is stored permanently in the LDAP/X.500 Directory Databases.

2) They then go through the Verification Process, which is the same as the Enrollment Process. From here, the Verification Template is created.

109

3) At this point, the Enrollment and the Verification Templates are created to form what is known as the "Master Biometric Template". The two are first matched, and a successful match is recorded into the PAM Server. The Master Biometric Template is also stored in the LDAP/X.500 Directories.

4) Suppose now the end user (or the employee) wishes to gain access to the Shared Resources Server. All they have to do is click on the appropriate icon onto their device. This will then trigger the following process to occur:

   ➢ After clicking on the icon, this will transmit a signal to the Authentication Server that a request is being made to access the Shared Resources Server.

   ➢ From here, the Quantum Key Distribution Center will issue the appropriate Public Key to encrypt the Master Biometric Template, which is already encased into another Data Packet, following the principles of Biocryptography, as detailed in Chapter 4.

   ➢ From here, the Authentication Server will transmit a message to the PAM Server to send the credentials to the Shared Resources Server, so that Authorization can happen immediately.

   ➢ The Master Biometric Template will also be transmitted to the Shared Resources Server as well, and in this transmission process, the Photon Particle Array Structure will protect the integrity of the Master Biometric Template.

   ➢ At this point, the Master Biometric Template will also be decrypted by the Shared Resources Server, by making use of the proper Private Key, which is also issued by the Quantum Key Distribution Center.

It is important to note at this point that that even though the PAM Server can instruct the Shared Resources Server to grant access, the Encryption/Decryption process of the Master Biometric Template also serves as another, or redundant Authentication check.

CHAPTER 6: Conclusions

Overall, this book has covered the theme of what the Zero Trust Framework is all about, as well as its limitations and advantages. The Cyber Threat Landscape is changing at a very fast pace, and thus, it is very important to try to keep up as much as possible. Other security solutions have been tried and for the most part have failed, especially that of the Perimeter Defense Model, which was also reviewed in detail in this book.

We need a newer solution that is unique, cutting edge, as well as scalable for the long term. This is where the Zero Trust Framework comes into play. This has been viewed as an extreme sort of methodology by both society and business, because in it, nobody can be trusted whatsoever, from either the internal or the external environments. But wherever it has been deployed, there has been some proven success with it, as it has helped to greatly reduce the statistical probability of being impacted by a Cyberattack.

But even here, the Zero Trust Framework is not without its own set of flaws, especially in the following areas:

> ➢ Still using hackable forms of Multifactor Authentication (MFA);

> ➢ The repeated need to be authenticated over and over again;

> ➢ The possibilities of having the information and data transmitted from the Authentication Server to the Shared Resources Server being tampered with, and the integrity compromised.

We offered three distinct solutions for these flaws, which are as follows:

> ➢ Making use of Biometrics as the only form of MFA tools. In this regard, the use of Fingerprint Recognition, Iris Recognition, and Facial Recognition were introduced.

> ➢ The use of Privileged Access Management (PAM) as an alternative to avoid having to be authenticated and authorized over and over again.

> ➢ Making use of the concepts of Quantum Mechanics and Quantum Cryptography as a means to protect the integrity of the transmissions from the Authentication Server to the Shared Resources Server.

At this point, it is important to review the highlights of what was covered in each chapter of this book:

Chapter 2:

> ➢ A History Into Cryptography

> ➢ The Evolution of Cryptography to Present Day Uses

> ➢ A Review of Encryption, Decryption, Hashing, and Digital Signatures

➢ Our Proposed Zero Trust Framework Model

It is important to keep in mind as well that the Zero Trust Framework is not a "one size fits all" solution. Instead, as its name points, it is merely a framework from which a business has to fit, mold, and adapt to its own security requirements and environment. In other words, what works for one organization will not necessarily work for the other. Therefore, a lot of time and planning has to take place on the Zero Trust Framework that is most appropriate for you and your employees.

Speaking of which, apart from deploying the Zero Trust Framework in preplanned stages, it is also very important that you get the buy-in from your employees. After all, in the end, change is something that most humans don't like to endure, and because of that, you need to have an open lines of communications with them as each step of your Zero Trust Framework is being deployed. If you do not get their buy in, they will be very hesitant to use it (or not even use it at all), thus defeating its purpose entirely. Not just your employees, but every key stakeholder involved in your company must be informed as well.

Always be patient with the deployment of your Zero Trust Framework Model. It won't happen overnight, and in fact, if it is planned properly, it can take as long as a year until (or even more) it is fully deployed.

Finally, the question that gets asked is if one day the Zero Trust Framework will make the password obsolete. The password has been around for quite a long time, and it never seems like it will go away in the long term. But the potential for this to happen does exist, and technology is even available today to make this a reality, as was discussed throughout this book with the use of Biometric Technology. In the end, it all comes down to how much society really wants to change and improve their current levels of security.

As just stated, humans are by nature, very resistant to change, and are happy staying with the status quo, even if that change is for something better. This is the main hurdle that will need to be overcome if we are truly destined to become a password-less society. The tools are in place – we just have to see the benefits of it and accept it in the end.