THE PENNSYLVANIA STATE UNIVERSITY

SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

CYBERSECURITY – AN ANALYSIS OF BIOMETRIC IDENTIFICATION RISK FACTORS IN THE CYBER DOMAIN

MAXIMILLIAN ALEXIS FIGUEROA

SPRING 2021

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Security and Risk Analysis - Cyber Security
with honors in Security and
Risk Analysis - Cyber Security

Reviewed and approved* by the following:

Rhoda Joseph
Associate Professor of Information Systems
Thesis Supervisor

Andrew Morrow
Lecturer in Information Sciences and Technology
Faculty Reader

David Witwer
Director of Capital College Honors
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

Biometric technology is taking over the cyber domain. Layered security such as passwords, usernames, and pin numbers are moving toward the reality of becoming things of the past. With how fast technology evolves, it is likely to assume that layered security will become entirely obsolete and biometric security will become the only reliable form of digital security left. With such a high dependency on a single form of security, there will be risks, vulnerabilities, and someone who wants unauthorized access to the data it's protecting. This study will define the use of biometrics and cover their many variants. It will also focus on the possible vulnerabilities leading to the imminent theft of classified or personal information, resulting in a cyber-attack that could potentially cause irreversible damage. Biometric identification theft poses an even greater risk than that of a password or PIN number being compromised because it is configured by the genetic make-up of the end-user. Which not only contains the data being secured, but also personal information in thorough detail about the end-user. This study will exploit the gap between public trust in biometric encryption and the risk factors of its implementation in today's modern devices. Which led to one of the largest biometric breaches in American history at the United States federal Office of Personnel Management (OPM).

TABLE CONTENTS

LIST OF FIGUERES

LIST OF TABLES

ACKNOWLEDGEMENTS

Thank you to my family and readers Dr. Rhoda Joseph and Professor Andrew Morrow

Ch. 1

Introduction

Technology is an ever-growing field; it is used in construction, law enforcement, finance, science, environmentalism, medicine, and much more. Above all, it is used for gathering and storing information. It is likely to assume that some companies would cease to exist without information. The loss or theft of information could have detrimental effects on employees or the company's survival. Therefore, information is incredibly valuable. However, just like anything that has value, there will always be the threat of entities attempting to illegally exploit vulnerabilities and compromise information. How do we mitigate such vulnerabilities to defend ourselves against these entities? Many believe that the answer lies within Biometrics. Biometric technology is taking over the cyber domain. Layered security such as passwords, usernames, and pin numbers are moving toward the reality of becoming things of the past. With how fast technology evolves, experts have theorized that layered security will become entirely obsolete and biometric security will become the only reliable form of digital security left.

With such a high dependency on a single form of security there is bound to be risks. Those risks pertain to the fact that manufacturers of biometric security systems are providing the end-user with a false sense of security. Research, interviews, and previous cybersecurity breaches have shown that biometric systems should not become the only form of security for deterring against a cyber-attack. Manufacturers have misled the end-user to believe that accurate authentication is the equivalent of sustaining a secure system. A device is not secure simply because the user is authenticated. The purpose of the following research intends to prove these statements, in an effort to strengthen the security procedures Developers and Project Managers

take prior to implementing a new biometric system. These procedures will consist of exercising cryptanalytic penetration tests. This is when a corporation attempts to breach its own system in a scenario-based cyber-attack. Implementing cryptanalysis before the launch of a biometric device will mitigate the vulnerabilities of biometric systems. Thus, strengthening the security of biometrics and ultimately resulting in an increase of efficiency in cybersecurity.

The intended outcome for solving this question is to increase digital security in the precipitous field of biometrics. Doing so, will safeguard personal information, financial data, as well as classified or even top-secret federal records. Information will be gathered based on research databases and sources that provide expert knowledge in the field of cybersecurity. The analysis will also cover why students play a key role in biometrics. Students use biometrics every day, from accessing their smartphones, laptops, and bank apps. They are also one of the primary targets for marketing in the biometric field. One of the many goals of this analysis is to challenge the audience, by raising to awareness to questions such as: what is Cryptography, what is Cryptanalysis, what is the difference between the two fields, how often are they used in biometrics, and above all, can biometrics be trusted? Answering these questions will reveal that there is a knowledge gap in security, between the manufactures of biometrics and the consumers who use them. A false sense of security is a misunderstanding. This misunderstanding will not only reveal the gap mentioned previously, but also a technological gap between Cryptography and Cryptanalysis, which will both be defined in chapters two and three.

Another form of analysis will also come from a Cyber Threat Map. A Cyber Threat Map is a map of worldwide cyber attacks being launched in real-time by none other than, cyber criminals themselves. There are many forms of threat maps to choose from, many of which that are not sponsored by the Department of Defense or other federal agencies. For the sake of

credibility and accuracy in research, this analysis will be conducted using the Cyber Threat Map from world renowned anti-virus software company, Kaspersky. Cyber attacks are talked about everyday and shown to the public in multiple ways, from TED Talks, statistics, interviews with experts, and commercials on TV. While this may, make sense to security experts, all this media and data can leave those who aren't familiar with technology feeling very confused. Most people comprehend that computers are a part of everyday life and are at risk of being attacked.

However, when it comes to understanding hard numbers and raw data, most people cannot mentally picture how detrimental these attacks truly are and what those numbers really mean. This is due to fact that cyber-attacks are unique in such a way, that these attacks cannot be physically seen, they are only digitally viewable. Also, predators do not have to wait for the right time to launch an attack. Hiding in the dead of night and waiting for the right moment to strike is a thing of the past. Cyber-attacks are launched every minute of every day and are indiscriminate of gender and race. The use of a Cyber Threat Map will allow even the most non-technologically affluent individual to understand how prominent cyber-attacks are, by allowing the viewer to graphically visualize how many attacks are launched per day. The purpose of showing this is to ultimately bridge the gap mentally and visually between understanding the rapacious growth of cyber theft and how biometrics need to be as secure as possible to endure such an overwhelming number of attacks. Doing this, will raise the urgency and awareness of the issue in biometrics.

Ch. 2

Literature Review

History of Biometrics

Biometric technology is taking over the cyber domain. Layered security such as passwords, usernames, and pin numbers are moving toward the reality of becoming things of the past. With how fast technology evolves, it is likely to assume that layered security will become entirely obsolete and biometric security will become the only reliable form of digital security left. With such a high dependency on a single form of security, there are bound to be risks, vulnerabilities, and someone who wants to access the data it is protecting. Biometric security is believed to be one of the most advanced and trusted methods of cybersecurity ever created. It can be found everywhere from smartphones, airport security, cars, schools, government databases, buildings, bank vaults, and even blood banks. But what are biometrics?

While there have been many different definitions in the past, Dr. Nitzan Lebovic (2015) in *Biometrics, or The Power of the Radical Center* from the University of California explains the history of biometrics and defines them as the "archiving of biological data based on the surveillance and control of bodily images". But before bodily images and biological data were quantified, the study of Metrics was the first method of bringing about the possibility of measuring objects and receiving numerical data. It was only until the 19th century that the concept of quantifying human forms was established. By the 20th century, the terms *bio* and *metrics* were joined together as a single form of study (Lebovic, 2015). Finally, in 1901 Francis Galton "identified the consistent use of measurement of body parts as randomly selected

numbers to generate large numerical claims" (Lebovic, 2015). Coincidentally, information such as this was useful to the prison and judicial system. Whether Galton knew it or not, this would become the first step toward biometrics being used for security purposes. With the ability to consistently measure body parts as segments of code, biometrics would soon begin their transition toward being used for Cryptography. The Oxford English Dictionary defines Cryptography as "The art or practice of writing in code or cipher; the science of encryption; the branch of cryptology… more generally: the study of codes and ciphers; cryptology". In essence, it is the study of secure communication by means of encryption. Encryption begins with ciphertext. Ciphertext is created by changing or modifying plaintext information into unreadable raw data. In summary, end-user information is encrypted into ciphertext and is therefore hidden. A thorough breakdown of the details behind the process of biometric encryption and how biometric technology itself is encrypted, will be explained in chapter three. For now, the analysis will continue to focus on the historical progression.

Since the discovery of biometrics having a role in security, Developers and Project Managers alike, have been implementing biometrics into almost all advanced security systems known to the 21st century. In the cyber domain, biometrics fall under authentication which is part of maintaining confidentiality. There are three different categories of user authentication, passwords and PIN numbers are assigned to the "what you know" category. Physical keys, smart cards, and mobile devices are assigned to the "what you have" category. Biometrics of any kind that involves human bodily features, including voice-recognition and signatures are categorized as "what you possess" (Kim et al., 2016). While biometrics may be a single field of study, as listed earlier there are numerous variants of their design. Physical and Behavioral biometrics are the two categories that distinguish what type of design the biometric technology is. Any form of

biometric technology such as facial recognition, retinal scanning, or fingerprints that rely on an individual's bodily features or characteristics are considered *physical*. Biometrics such as typing/key-stroke recognition or voice-printing are considered *behavioral* (Ngugi et al., 2011). Having the ability to turn such aspects of the human body into a means of securing and locking information is a very advanced concept to grasp; as well as it is unique. Unique and advanced, are two traits that the fields of cryptography and security are looking for. Which explains why biometrics have become so popular in their use of today's technology.

Types of Biometrics

Popularity with new technology is not uncommon. The applicability of biometrics has many uses outside the realm of security. Uses that wouldn't cause vulnerabilities to privately secured data. Heart rate monitors on smart phones, voice-recognition messaging for safe driving, and retinal/cornea scanning for those who are visually impaired. These are all valid examples of biometrics that cannot perniciously impact the end-user's data. The issue of creating vulnerabilities presents itself when new technology is used as a means of security. Historically, research has shown that public trust in biometrics was lacking. An earlier study from 2002 shown in table 2-1 from the National Center for State Courts, found that the user acceptance rate for the approval of biometrics did not meet expectations (Ngugi et al., 2011). With only a handful of three-star ratings and no four-star ratings, user acceptance rate for biometrics was scarce, when being considered as a trusted method of security.

Biometric	Security Level	Accuracy	User Acceptance	Non-Invasive	Hardware
Fingerprint	***	****	**	***	Special, Inexpensive
Facial Recognition	**	***	**	****	Common, Inexpensive
Hand Geometric	**	***	**	****	Special, Mid-price
Speaker Recognition	**	**	***	****	Common, Inexpensive
Iris Scan	***	****	**	****	Special, Expensive
Retinal Scan	***	****	**	*	Special, Expensive
Signature	**	**	**	****	Special, Mid-price
Keystroke recognition	**	*	***	****	Common, Inexpensive
DNA	****	****	*	*	Special, Mid-price

Table 2-1: Types of Biometrics - National Center for State Courts

During that time, it was likely to assume that the implementation of biometric security would have only declined throughout the years, but that's simply not the case. Contrary to the data found in 2002, nineteen years later biometric technology can be seen everywhere in our devices, securing our private data. This raises many questions, but one in particular stand's out amongst others. Why is it that evidence of an increase in user acceptance of biometric implementation can be seen modern day; even though past data clearly showed a lack of confidence? One would assume that the answer must lie within how fast improvements are made to technology, given the number of years. However, that assumption would imply that fingerprint and retinal scanning needed improvements in 2002. It's not at all uncommon for technology to

require an update, but how is it possible that fingerprint and retinal scanning scored a perfect four-star rating in 2002, when tested on their accuracy nineteen years ago? Surely, the amount of work that has been done on biometric technology since then required more than just an update. This leads to the conclusion that society is becoming more reliant on biometric accuracy and acceptant of biometric security, under the stereotypical assumption that technology becomes progressively better throughout the years. Which exposes the public to a plethora of vulnerabilities by providing a false sense of security. This statement can be proven by understanding the following attributes that led to this false sense of security.

Ch. 3

Analysis of Biometric Risk Factors

Cryptography and Cryptanalysis

An interview was conducted with experts such as Richard Clark, a former White House advisor of several U.S. presidents who worked in the field of cybersecurity. He explains that new technologies are notorious for being insecure, which become gateways for terrorists and non-state actors to launch a cyber-attack (Clarke, 2017). Many experts like Clarke have cautioned against the imminent threat of a large-scale cyber-attack. Clarke warns that just because a large-scale cyber-attack hasn't happened yet, that doesn't mean it never will. When asked about whether or not this imminent threat is acknowledged; Clarke replied with:

> I do think that U.S. leaders...understand the magnitude of the threat and the potential damage that cyber threats can inflict on our country, but they haven't yet acted on it. I believe it isn't clear to many of them exactly what action to take.

Biometrics have yet to become a guaranteed method of safeguarding data. As stated previously, new technologies are insecure, meaning that they are breakable and open for attack. Ngugi states "Biometrics are new technologies that have not been well explored… Biometric researchers believe that biometric technologies have the potential to become an irreplaceable part of authentication systems" (2011). Meaning that experts speculate its future role in the field of cybersecurity will only continue to grow. Layered security such as password and username will become security methods that are practiced moderately or quite possibly – not at all.

A false sense of security is the ultimate reason society continues to move ineluctably toward a digital future of risks. Recalling table 2-1, accuracy and security are relatively high in both categories of fingerprint and eye scanning, at a four-star rating. While user acceptance is at a two-star rating. Most would believe that high accuracy and security would be positive traits. They are – however, accuracy is not the equivalent of security. Hence the reason of why security and accuracy are separated into two different categories. Therefore, they are two different fields that yield very different results when being applied to cybersecurity. Cryptography focuses on encryption and encoding of data, which provides the accuracy and authentication. Cryptanalysis, which focuses on actively attempting to break or breach the encrypted code, provides the security. The Oxford English Dictionary defines Cryptanalysis as "The analysis and decryption of encrypted text or information without prior knowledge of the keys; (also) the science or study of this" and a Cryptanalyst as "An expert or specialist in cryptanalysis; a person who deciphers encrypted information".

Understanding what each field specializes in is important because it means that even though many companies and manufacturers of biometrics strive for the most accurate hardware, they're still only working within one scope of the field, which only focuses on authentication. This limits their means of security and because accuracy provides no security from a cyber-attack, this leaves data that is biometrically encrypted vulnerable to such attacks. Overestimating how secure new technology will be, as well as not having a full understanding of both Cryptography and Cryptanalysis has attributed to the risk of biometrics being attacked. The question then becomes, if the data is vulnerable to attacks, what are the potential avenues of attack? The answer lies within the process of how the user's biometric data is encrypted.

Biometric Encryption

The following example provided by *Precise Biometrics*, will assume that fingerprint biometrics are being used, primarily because they are the most implemented and arguably the most secure.

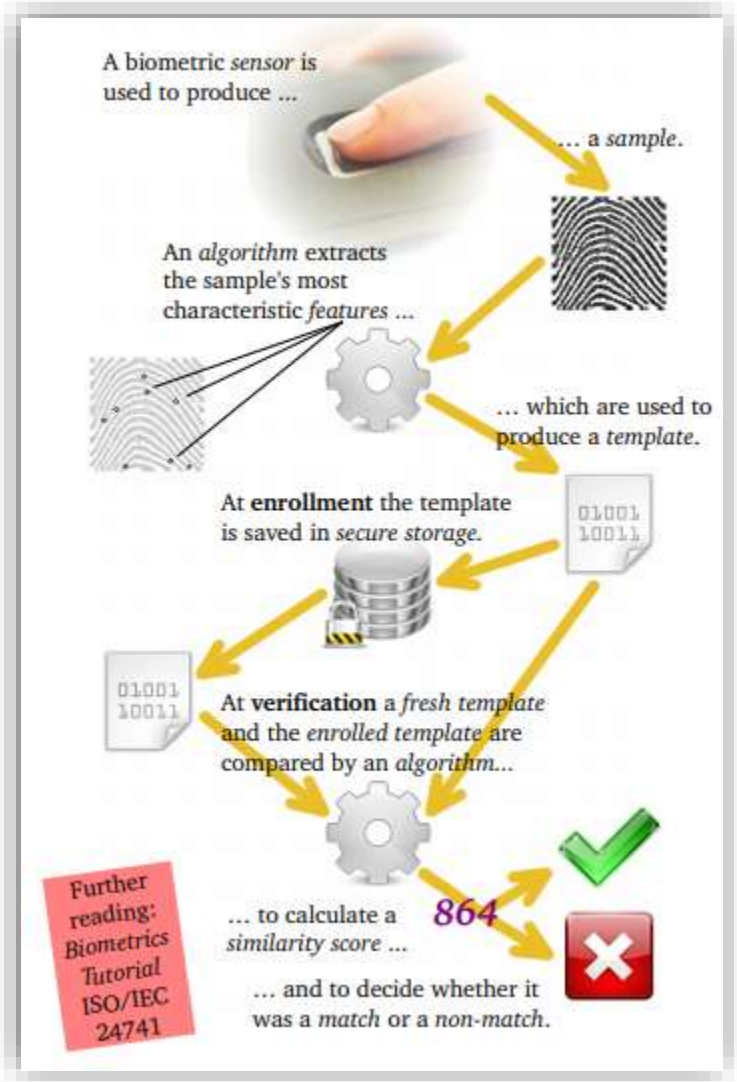

Figure 3-1: Biometric Fundamentals

Figure 3-1 only provides a general explanation of procedures used in biometrics to secure the end user's information. For clarity, Figure 3-1 will be broken down into the following steps:

Step 1: A biometric sensor is used to create a sample of the fingerprint.

Step 2: An algorithm extracts defining features to create a biometric template.

Step 3: The template is enrolled and saved to a secure storge location within the computer.

Step 4: The user attempts to authenticate themselves, the fresh template is compared to the previously enrolled and stored template.

Step 5: Error tolerance is calculated to generate a *similarity score* that is like the previously stored score, resulting in a *match* or *non-match*.

With a focus primarily on step five, the Biometric Error graph in Figure 3-2 shows this step in greater detail (Conrad et al., 2017).

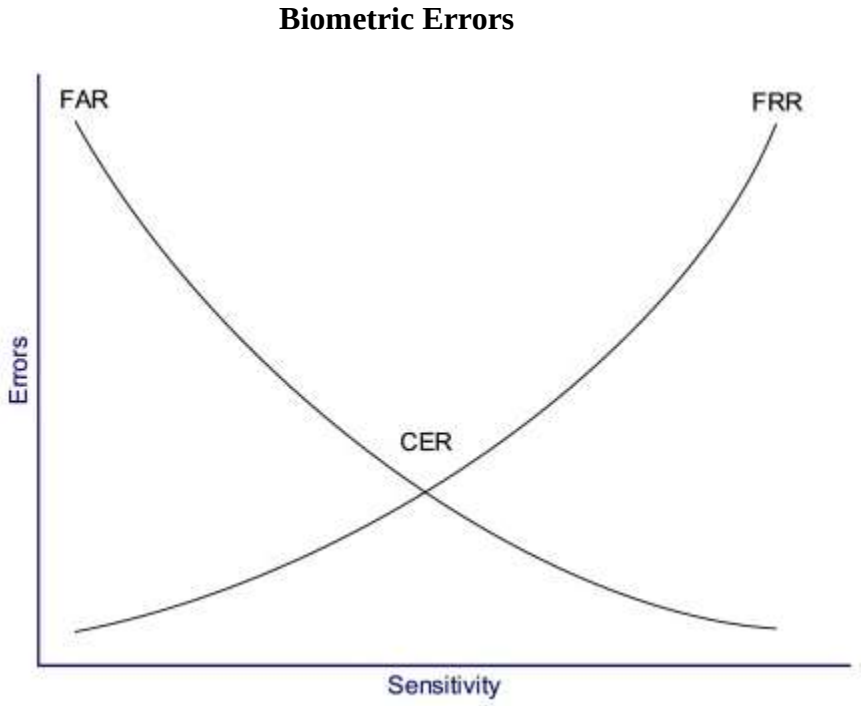

Figure 3-2: Biometric Error Graph

Step one is fairly simple to understand, an authorized user has placed their finger on the biometric device to authenticate themselves, thus gaining authorization to the data that was encrypted by the biometric device. Step two is where manufacturers work diligently, while striving to achieve the most accurate authentication for the user via the biometric device, to ensure that only the correct user gains access to the data. But how is this accuracy achieved? The biometric device scans and measures the distance between each individual print on the user's finger and then converts the measurements into numerical data to create a *biometric template* (Conrad et al., 2017). With the template enrolled and saved in the system's storage, the same user attempts to reauthenticate themselves in step four. Figure 3-2 demonstrates the behavior of the biometric system in step five, when it compares the new template to the previously enrolled template.

To understand the graph, one must have a thorough understanding of biometric errors. Beginning with the False Rejection Rate (FRR), this error causes many frustrations to Developers and Project Managers. It denies access to those who should rightfully have access to the data or system. The user attempts to authenticate themselves to the system, however, their fingerprint is either wet or dirty. Due to the distortion of the fingerprint, the system denies the user. This is known as a *type 1 error* (Conrad et al., 2017). The next form of error is the False Acceptance Rate (FAR). Possibly one of the most dangerous types of errors known to security experts, the FAR error authenticates and grants access to an entity that should not have access to the data. This is known as a *type 2 error* (Conrad et al., 2017). Both types of errors are controlled by the biometric sensor's sensitivity level. If the sensitivity for the sensor is too low, then users who are unauthorized will gain access to the system, putting both the confidentiality and integrity of the data at risk. However, if Developers try to increase the sensitivity, then they risk

locking themselves out of their own system, which compromises availability. Therefore, those who oversee the deployment of a new biometric device are forced to keep the sensitivity low. In step 5, the end-user's first similarity score will not match the next, or any others again. This is because the data captured from a fingerprint, can be compared to a signature. No two signatures are the same, both are unique in their own way even if they look similar. Which means that the similarity score must leave room for error (Conrad et al., 2017). It is up to those who Developers and Project Managers to decide how much error will the biometric device be willing to tolerate. This is the risk of using biometrics. Fortunately, those who oversee biometrics are aware of this risk and combat it with the Crossover Error Rate (CER). The CER is at the point of intersection between both graphs, where the sensitivity has been adjusted so that it is not high enough to lock out the end user, but not low enough to allow unauthorized users (Conrad et al., 2017).

State-of-the-art encryption yields definitively accurate results. Which in turn greatly reduces the probability of unauthorized access to private or sensitive information, thus providing security. While this form of logic may seem true from the perspective of Cryptography and accuracy, it is false within the field of Cryptanalysis and security. The feeling of security given to the end user provided by a successful biometric scan is, in fact, the false sense of security mentioned previously. The ability of authenticating a user-identity with strict precision does not constitute the protection against a cyber-attack. Nor does it make the identifying template any less susceptible to an attack than that of a standard computer file. This is because the security of the template, lies within step three, where the template should be stored in a secure location. Whether or not a user is able to authenticate themselves in their device is irrelevant to a hacker. Cyber-criminals target the location of the template itself and actively attempt to penetrate whatever defenses are protecting it.

Biometric Marketing

Marketing has made biometrics incredibly trustworthy by introducing biometric technology to smart phones. This was an excellent strategy from a marketing perspective. Anything which requires a username, password, or pin number for authentication automatically becomes a candidate for biometric technology. Furthermore, due to the reasons stated previously, the end-user subsequently trusts the biometric technology without fully comprehending the amount of risk that comes with using biometrics. Consequently, biometric encryption is only as secure against a cyber-attack as the end-user believes it to be. Thus, creating a false sense of trust within the end-user. Of course, the first step to solving any problem is figuring where the root of the problem lies. While it is true that the project manager responsible for deploying these technologies may have no other choice but to expedite the project in order to meet budget, public, and stakeholder demands, the problem may stem deeper than just management (Pahker, 2019). The primary issue which links marketing and technological ignorance together isn't just from application developers who must meet a timely quota. The issue also stems from the stakeholders themselves who believe that improvements can be made later. Anna-Kati Pahker of a leading software company called *GANTTIC* which provides project management tools, states "While completing the project fast and within the budget might bring the project manager personal gains, overlooking security doesn't. That's on the stakeholders" (2019). If stakeholders are not serious about making security their top priority, this puts pressure on the project manager, leaving little room for implementing proper security procedures.

Thus, the biometric-enabled device is then released to the public with unsustainable solutions to cyber-attacks. With fingerprint biometrics on the rise, this puts the public at risk. Students carry electronic devices every day that have biometric features, commonly used items

such as smart phones and laptops come with fingerprint sensors and even facial-recognition already built in. Consumers are indulging in the convenience of biometrics, after all, biometrics completely eliminate the requirement of remembering a username and password. Even biometric researchers agree, stating "Besides, biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for variety of applications" (Kim et al., 2016). But at what cost? The cost of having biometric data stolen is steep. Alison Grace, an author from leading antivirus software company *Norton,* states "Biometrics may become so commonplace that people become complacent. They might not use the kind of common-sense security measures that they use today because they think that biometrics will solve all of their security problems" (2019).

Grace continues to explain one of the greatest threats in biometrics – theft. While a benefit of biometrics may be that they're easy to use, the risk is that once the biometric data is compromised, it cannot be changed. On the topic of the difference between biometric theft and password theft, Grace says "The data stored in a biometric database may be more vulnerable than any other kind of data. You can change passwords. You can't change your fingerprint or iris scan. This means that once your biometric data has been compromised, it may no longer be in your control" (2019). Jeremy Erikson, an author from trusted Penn State security software company *DUO* says:

> FRR of 7.5% and FAR of 0.1% is often cited, typically based on a small sample of less than 1000 test cases. However, other studies estimate the FAR rates to be much higher. This is, at best, an order of magnitude worse than the FAR rate of 0.01% that FIDO sets as a standard. Unfortunately, when it comes to electronic fingerprint scanners, there does not appear to be *any* publicly-available data on the FAR and FRR rates. But let us assume that the FAR rate is sufficient to generally prevent accidental unauthorized device unlocking and look adversarially [*sic*] at fingerprint scanners.

Erikson is saying that just because there is no way of universally tracking how many errors occur during a biometric scan, that doesn't mean that they don't occur at all. While fingerprint FAR errors only make up 0.01% of errors, biometrics should still be approached with caution if the user intends to encrypt their data (Erickson, 2020). Author Nils Matthiesen has published over 40 articles in the field of cybersecurity, and recognizes that the chance of an FAR error is low. However, he warns that:

> Despite the advanced technology, no biometric process is 100% secure. While the error rates are low (see above), the systems need to allow for measurement tolerances based on the fact that with all the different measurements involved, your finger, eye, or signature never deliver exactly the same data because your eye or finger may be at a different angle. This means only a rough match can be determined. Furthermore, characteristics that can be identified biometrically are constantly changing – through ageing, illness, injury, or just through what life throws at you. Nevertheless, good biometric processes have a high recognition rate, particularly if the system modifies the reference model dynamically every time after it has recognized the individual in question.

Cryptanalysis procedures should be mandated and exercised before the technology is released to the general public. Unfortunately, the practice of cryptanalytic security is habitually placed after deployment of the product. As biometrics continue to move forward into the future, vulnerabilities such as overzealous marketing and technological complacency are becoming all too common. Evidence and warning signs are everywhere, pointing to the fact that we are leaving ourselves open to attack. Small cyber-attacks are continuously repeated because attackers are trying to breach the secure systems through trial and error. History has proven many times that small and consistent advances toward any goal, (good or bad) will eventually add up and ultimately result in at least one successful trial. Inefficient cryptanalysis, technological ignorance, and underestimation of small cyber-attacks are all indicating the threat of a large-scale cyber-attack. Consequently, every failed attempt brings hackers one step closer to success. The

repercussions of this technological complacency would soon catch up with the United Sates on June 4th of 2015.

OPM Data Breach

The United States federal Office of Personnel Management (OPM) fell victim to a large-scale cyber-attack, resulting in the confirmed theft of over 21.5 million governmental and employee information records and applications, in a 2015 report by *Biometric Technology Today*. Of the 21.5 million records, 5.6 million of them were biometric fingerprint templates. This information references what was covered in the step-by-step figure in chapter three and the remarks that were stated earlier on technological complacency. Step three, the biometric template should be enrolled and stored in a secure storage location. As stated previously, authentication means little to hackers, as their primary target is the location of where the biometric data is being stored. Once that is discovered, hackers will repeatedly assault the storage location within the computer, to illegally breach into and compromise the stored data.

It is still uncertain as to who or what hacked the OPM, however experts speculate that the source came from China (Biometric, 2015). The OPM had become complacent in their security practices, leading to millions of stolen personal data. In a news article by *Federal News Network*, it claims that "OPM's cybersecurity practices were woefully inadequate, which allowed hackers to access to the agency's storage of employee information, background investigation and security clearance data that exposed individuals to heightened risk of identity theft. [Officials] also claimed that given the time which has passed since the data breach, it is possible [victims] will suffer future harm "traceable" to the OPM data breach" (Brust & Thornton, 2019). One thing, however, is certain. If security officials are not doing their best to protect their systems from cyber-attacks, it doesn't matter how secure biometrics are. They will be hacked – history has

proven this. The security officials who oversee the implementation of biometric systems, must adhere to the warnings of their auditors. The analysis has proven that biometrics are not 100% secure in authentication, nor are they 100% secure in security and provided reasons as to why they never will be. While fingerprints may seem to be the most popular variant of biometric technology, recently another variant has been gaining attention.

Ch. 4

Biometrics and Law

Facial Recognition and Biometric Technology Moratorium Act of 2020

Facial-recognition biometrics have been gaining traction in their popularity. While biometrics differ from each other in terms of their use, they also differ from each other in terms of how much of a threat they pose. Fingerprint biometrics can be threatening because of how they're stored and their risks of being attacked. After the OPM was hacked, worrying about cyber-criminals would soon be the least of the public's concern. Every citizen in the United States must also be cautious of their own government. Allowing governmental security cameras and traffic cameras to be programmed with facial-recognition technology, adds a new threat to public privacy. Biometric researchers Eric Conrad, Seth Misenar, and Joshua Feldman are in agreeance, saying "*Facial scan* technology has greatly improved over the last few years" (2017). Followed by, "Although not frequently used for biometric authentication control due to the high cost, law enforcement, and security agencies use facial recognition and scanning technologies for biometric identification to improve security of high-valued, publicly accessible targets" (Conrad et al., 2017). Should the government and security agencies have the right to turn people into *publicly accessible targets*? How well has facial-recognition technology improved over the last few years?

Robert Julian-Borchak Williams would know, he became the first target in 2020 to be publicly accessible by faulty facial-recognition technology. In an article written by Kashmir Hill

of *The New York Times,* documented the story of Willams, who was sitting in his home until one day receiving a call from Detroit Police department. The department called to tell him that he was under arrest and to come into the station immediately. Given that he was innocent, he thought it was a joke and left to go about his day (Hill, 2020). An hour later, when he returned home, he was approached by two officers who had been waiting for him on his front lawn, he was handcuffed in front of his family and driven to a detention center where he would have his mug shot and fingerprints taken. The facial-recognition software had falsely matched his driver's license photo to the security footage of a shoplifter (Hill, 2020). Alison Grace says "Laws governing biometrics are a work in progress, meaning your rights might be different from state to state. However, federal lawmakers may eventually create a cohesive law to address biometric privacy". Laws and especially facial-recognition technology, are a work in progress indeed. Something has to be done about this.

In June of 2020 federal lawmakers did introduce a new bill that would finally address the issue of faulty facial-recognition software. The Facial Recognition and Biometric Technology Moratorium Act of 2020 states that it is a bill "To prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance". While this is amazing news for public privacy and public safety, this only addresses one form of biometrics and the bill itself has yet to be passed. The issue with technology and law, is that new technologies like biometrics, are deployed and implemented faster than lawmakers can write bills. This unfortunately leaves room for future incidents to occur, that will also be unjust and unlawful. Which brings the analysis to the final question of: How can the end-user protect themselves from the vulnerabilities of biometric systems?

Ch. 5

Conclusion

Protection from Biometrics

The analysis has covered definitions, benefits, risks, laws, and expert opinions, but how does the public protect themselves? The easy answer would be to avoid using biometrics all together. While that is technically an option, it is unrealistic. Some jobs or careers require biometrics in order to gain access to particular areas or to log in to an account. Protection from biometrics must come from the decisions made by both the end-user and the project manager. The OPM hack had compromised security clearances and social security numbers. At the time, the millions of people whom it affected, would have never thought that their data was insecure. The point is, no matter how safe the user tries to go about using biometrics, there will always be the risk of identity theft because the security of their information ultimately lies within the hands of the company they work for. Thus, the first step toward protection in regard to what the end-user can do, is research the company's security policies and ask questions about what the company is doing to protect their employee's biometric data, as well as their regular data. Research the reputation of the company, the user should look for any data breaches that the company has experienced in the past, if any. If data breaches show up in the company's history, it would behoove the user to discover why and how it happened. Also, what has the company done since then to make sure that a data breach such as the one previously found, doesn't happen again. The user should also ask, how aware are the other employees about cybersecurity awareness training? This will reveal if the company has been distributing proper cyber awareness

training. Finally, the user can ask if there are options for logging in, other than biometrics. Such as username and password, with the additional security of two-factor authentication via phone text or app confirmation.

From the prospective of the project manager, what happened to the OPM says a lot about the dangers of what could happen when management becomes complacent about security. All biometric data, including other forms of data were stored only within the OPM. But that wasn't the only way data could be stored. Data can be stored in multiple locations, in order to improve the security of the data (Kim et al., 2016). For example, the biometric templet can be divided and stored in separate locations. Part of it can be stored with the company's systems and the other part can be stored on the user's laptop (Kim et al., 2016). This increases security, because if a hacker were to successfully break into a system, they would only have half of the biometric template. In other words, they would have to break into the company's system and the user's laptop in order to successfully compromise the full biometric template (Kim et al., 2016). This is no excuse for why this method of security wasn't implemented at the OPM, other than complacency.

As stated earlier in chapter three, the project manager isn't always the one to blame, if the stakeholders are not prioritizing security, then they make it exceedingly difficult for project managers to implement the proper security for the company. Anna-Kati Pahker says "it isn't really the project manager's job to sell the stakeholders on security" (2019). While this is true, at the end of the day, proper security of a company is everyone's responsibility. Project managers should make the extra effort to persuade stakeholders to reconsider how important cybersecurity is and how it will positively affect their investments in the overtime. Another commonly asked question about biometrics is: can a biometric identity be replicated by 3D printing or voice

recording? Unfortunately, research shows that the answer is – Yes. Nils Matthiesen calls this "Cloning", and says:

> It's difficult, but not impossible. Jan Krissler – who also goes by his hacker pseudonym Starbug – has succeeded in duping virtually every biometric process out there. He pulled off his most spectacular coup in 2014 when he created a fingerprint of Germany's Secretary of Defense Ursula von der Leyen based on a high-res photo of her. He even managed to fool the fingerprint sensor on an iPhone with a spoof fingerprint made from wood glue, and he used a fake hand made from beeswax to overcome high-security entry points that employ hand-vein scanners.

And Alison Grace from *Norton* says:

> Some pieces of your physical identity can be duplicated. For example, a criminal can take a high-resolution photo of your ear from afar or copy your fingerprints from a glass you leave at a cafe. This information could potentially be used to hack into your devices or accounts.

However, one should take into account, that a hack requiring the replication of an actual bodily feature takes incredibly large amounts of resources, time, and effort. Not all cyber-criminals have access to all three. In conclusion, security will never be perfect, nor can it be 100% guaranteed. But it can be better and more effective when communication is clear. Security works best when everyone practices it together. While biometrics may pose an imminent threat, the bill mentioned in chapter four, provides hope for the future of security, knowing that lawmakers are aware of how dangerous biometrics can be.

REFERANCES

Biometric Technology. (2015). OPM hack now stands at 5.6m fingerprints. *Biometric Technology Today*, *2015*(10), 1–2. https://doi.org/10.1016/s0969-4765(15)30145-4

Brust, A., & Thornton, D. (2019, June 27). *Appeals court rules OPM data breach left people vulnerable to harm*. Federal News Network. https://federalnewsnetwork.com/workforce/2019/06/appeals-court-rules-opm-data-breach-left-people-vulnerable-to-harm/.

Clarke, R. (2017, June 29). *The Risk of Cyber War and Cyber Terrorism*. JIA SIPA. https://jia.sipa.columbia.edu/risk-cyber-war-and-cyber-terrorism.

Conrad, E., Misenar, S., Feldman, J., & Simon, B. (2017). *Eleventh hour Cissp: study guide*. Syngress, an imprint of Elsevier.

Erickson, J., & Engineer, S. R. D. (2020, March 11). *The Good and Bad of Biometrics*. Duo Security. https://duo.com/labs/research/the-good-and-bad-of-biometrics.

Grace, A. (2019). *Biometrics and biometric data: What is it and is it secure?* Official Site. https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html.

Hill, K. (2020, June 24). *Wrongfully Accused by an Algorithm*. The New York Times. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Kim, H., Jeon, W., Lee, K., Lee, Y., & Won, D. (2016). Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme. *PLOS ONE, 11*(2). https://doi.org/10.1371/journal.pone.0149173

Lebovic, N. (2015). Biometrics, or The Power of the Radical Center. *Critical Inquiry, 41*(4), 841–868. https://doi.org/10.1086/681788

Matthiesen, N. (2021, March 17). *Biometrics really are (in)secure*. Avira Blog. https://www.avira.com/en/blog/biometrics-really-are-insecure.

Ngugi, B., Kamis, A., & Tremaine, M. (2011). Intention to use biometric systems. *e-Service Journal, 7*(3), 20. https://doi.org/10.2979/eservicej.7.3.20

Pahker, A.-K. (2019). *Are Project Managers to Blame for Software Security Threats?* Ganttic. https://www.ganttic.com/blog/project-managers-software-security.

Precise Biometrics. (2014). *Understanding Biometric Performance Evaluation*. https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation. (n.d.). https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation.pdf.

ACADEMIC VITA

Maximillian Figueroa

Education:

Bachelor of Science Degree in Security and Risk Analysis, The Pennsylvania State University, Spring 2021
Minor in Homeland Security
Honors in Security and Risk Analysis

Thesis Title: Cyber Security – An Analysis of Identification Risk Factors in the Cyber Domain

Thesis Supervisor: Dr. Rhoda Joseph
Faculty Reader: Andrew Morrow

Experience:

Deloitte: Cyber Solution Developer – Cyber and Strategic Risk Department
U.S. Army: Signal Corps Officer – 25A

Awards:

Dean's List
National Society of Leadership and Success
Chancellors Student Leadership Access Program
ROTC Top Cadet

Activities/Presentations:

President, Cyber Club, 2016-2017

Vice President, Community Service Club, 2017-2018

Cadet Captain, ROTC cadet summer training, 2019 – 2020