Surveying Security and Privacy of Biometric Authentication on Devices and Software

Final Report

Lead: Shivam Singh
University of Central Florida
Oviedo, FL United States
sh443844@ucf.edu

Phaneendra Allu
University of Central Florida
Oviedo, FL United States
ph677833@ucf.edu

Michael Cooksey
University of Central Florida
Longwood, FL United States
cookseymichael5@gmail.com

ABSTRACT

Authentication is a vital part of security as it lets us safeguard private information behind a security feature. However, authentication can be overcome by attackers. It is important to evaluate the security concerns surrounding authentication. While there are several ways to authenticate ourselves today, we will take a deeper look at how biometrics are used in authentication. This means we will discuss the overall security of biometric authentication and determine how secure it is by today's standards. We have accomplished this by conducting a survey of papers on biometric authentication and its security issues. In this paper, we will reveal all the significant findings from our survey and how they helped us meet our goal. The results will evaluate specific case studies and common attacks on biometric authentication. With this information, we will be able to draw our conclusions on biometric authentication security.

INTRODUCTION

Biometric authentication is the use of a biometric (iris, fingerprint, etc.) to securely authenticate a specific user to a digital system. For example, a user can unlock their iPhone using their own fingerprint. This security feature is used to access our data easily while still having an effective authentication feature in place. How effective is biometric authentication? This is a question we have asked ourselves and will discover throughout this study.

The way we will determine this is through a detailed survey of professional papers. The papers we collect will serve as a basis for our understanding of biometric authentication and pave the way for our discussions. We will also focus on three main biometrics fingerprints, irises, and facial features. The sections of this paper will identify each step we took and the problems we encountered. Our focus will be on individual case studies that show attacks and proposed solutions for biometric authentication. We will discuss our techniques, challenges, and results further, throughout the paper.

KEYWORDS

• Biometrics • Fingerprint • Facial Recognition • Iris Recognition • Security Mechanisms • Privacy • Evaluation Metrics • Spoofing • Template attacks • Data Simulation • Authentication • Vulnerability

1. PROBLEM STATEMENT

The advancements in the field of Biometrics have introduced a new means of authentication over the traditional mechanisms of utilizing PIN and password. This way of authentication uses unique physiological and behavioral traits referred to as biometrics. It is important to assess whether the technologies built on biometrics are strong enough to withstand various security attacks on our current systems in today's world. This survey analyzes the attacks possible at various levels and factors making it vulnerable to breaches on various biometric systems and an overview of mitigation procedures to evade the success of attacks.

2. RELATED WORK

Research involving facial, iris, and fingerprint recognition individually and in some form of combination has become multifaceted research. Each area has its dedicated scholars publishing great insights on how secure is a biometric-based authentication system which widely pre-assumed to be secure and private.

There has been significant research conducted recently on Facial Authentication Systems, primarily because of heavy investment in artificial intelligence and machine learning algorithms globally in the last decade. The main objective of ongoing research is to improve the accuracy and speed of the system when exposed to a dynamic background. Research groups are also putting great emphasis on making facial authentication systems increasingly more secure against attacks that use impersonation to fool the system. Furthermore, research on privacy aspects of facial authentication systems has also seen a lot of contribution over the last five years [30]. Interestingly researchers in the European region are dedicating their efforts towards making the authentication systems privacy compliant per the European Union rules and regulations.

Iris-based and fingerprint-based authentication systems still have researchers' interest as they see a huge scope in improving the security of the system against print or presentation attacks. A huge part of recently conducted research has in on how these two authentication systems can be integrated with another form of biometric-based authentication systems to make them more secure against trivial attacks. We have surveyed [18] which discusses how iris scanning acts as multi-factor authentication and significantly improves security along with the accuracy of the system.

3. SURVEY TECHNIQUE

3.1 APPROACH

To ensure the success of our literature survey, we adopted a combination of systematic and thematic reviews, shortlisting

research papers and then drawing our conclusions from them. Project 10 from fall'22 [11] and the journal on how to review research papers "How to Read a Paper" [12] made our survey technique very robust and greatly streamlined. We started searching for papers on Google Scholar, UCF Library, and security conferences listed on Jianying space with keywords from the earlier section. These keywords resulted in a wide variety of papers that covered a very wide domain and kept our survey focused. We had to eliminate papers that were beyond the scope of our course. The systematic approach facilitated the classification of research papers based on their context and implementation areas, ensuring high knowledge extraction and equitable work distribution.

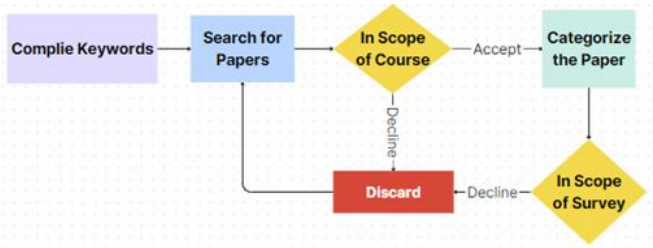

Fig 1: Flow for shortlisting paper for the survey

While categorizing the papers we used a three-pass approach, the first pass involved obtaining a high-level overview of each paper by addressing the five C's: Category, Context, Correctness, Contribution, and Clarity. This enabled us to decide whether to proceed with further passes or explore alternative references. The second pass aimed at grasping the paper's essence, summarizing results through graphs, diagrams, and illustrations. The final pass aimed to uncover hidden assumptions and shortcomings, jotting down key ideas for future work, thereby determining the paper's value in contributing to our survey. Additionally, we employed a thematic approach to align our survey's goal of identifying potential attack scenarios and determining whether current biometric authentication systems are secure enough or not.

3.2 RESULT EXAMINATION

We concluded the selection of a specific number of papers for inclusion in our survey and to enhance results. We designated one team member as the subject matter expert (SME) for each category. Each team member was assigned the task of reviewing one to two papers weekly and subsequently presenting a one-page summary to the team. The summary encompassed three key areas: Overview, Method/Attack, and Results. Following the completion of all presentations, the team engaged in a collective brainstorming session to identify flaws and discuss security mechanisms in the papers presented thus far. This approach fostered knowledge sharing and facilitated the extraction of effective conclusions from various sub-domains within the field of biometric authentication.

3.3 CHALLENGES

Despite our adherence to these techniques and processes, we encountered numerous challenges. To make this survey an efficient case study we are presenting all the challenges we faced:

1) Availability of research paper that applies to all forms of biometric authentication.

2) A huge overlap with other fields of science made it difficult to absorb the content to its full potential.

3) High Inter-linkage amongst all existing papers: Most researchers are adding on a different aspect of the same vulnerability. This limited the availability of variety in research papers.

4. ATTACKS

4.1 FACIAL AUTHENTICATION

Facial authentication refers to the use of a user's facial features to obtain valid access to a system [8]. This section will focus solely on attacks of this biometric authentication and their proposed mitigations.

4.1.1 DATA SIMULATION

Data simulation is an attack where an attacker creates a counterfeit of a valid input to fool a system and successfully bypasses the security mechanism. We reviewed "Attack Analysis of Face Recognition Authentication Systems Using Fast Gradient Sign Method" [13] which was shortlisted using our predefined survey technique. The paper describes how the Fast Gradient Sign Method can be utilized to simulate data to fool a facial recognition authentication system that uses a machine learning model. To understand the attack first we need to understand the loss function of any ML model. A loss function is a mathematical representation that maps the difference between a predicted and an actual value in any ML model. Now, the FGSM working model is by computing the gradient (slope) of the loss function concerning the input dataset and then by modifying the input dataset in a way that it cannot be noticed by a human eye. However, the model would be misled to make an incorrect classification or false prediction. After training the model with such modified data for some significant time, this attack can bypass the model and gain access to the system with a different person's face.

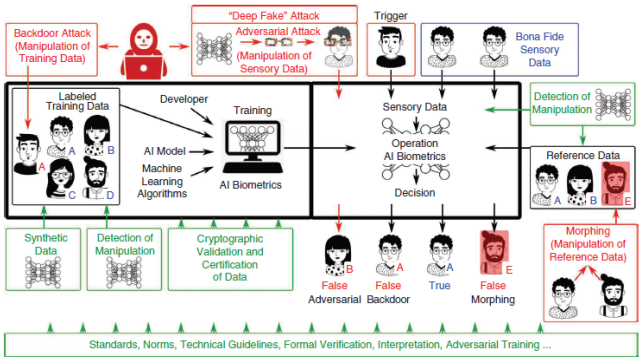

Fig 2: Attacking different aspects of the ML Model [14]

The author has mainly described two approaches to this attack, targeted FGSM and untargeted FGSM. In Targeted FGSM the

objective is to mislead the model so that it misclassifies a particular user and gets access to the system with modified data (Someone else's face). Whereas in untargeted FGSM objective is to let the model misclassify input data of the whole class to another class, but not the true class i.e., the image of any user's face can get access to the system as any other user but not as his own identity. Experiments have shown that the FGSM attack is very efficient in breaking the ML-based facial recognition authentication system. It has proved that the level of security of such a system is completely dependent on the training of the model because targeted FGSM can bring down the accuracy of the model from 98.38% to 85.17%. It is more astonishing to see that with untargeted FGSM the drop in accuracy of the model is very significant from 92.58% to 38.61%. This means that data simulation is a very strong attack on systems that use a data set to train the model for authenticating identity.

4.1.2 DATA POISONING

One would assume that developing an algorithm that has a better learning rate and exponentially increasing the number of epochs would safeguard the ML-based facial authentication system but "A New Facial Authentication Pitfall and Remedy in Web Services" [15] discusses how a well-trained and efficient algorithm be broken with data poisoning. The paper discusses how the attackers infiltrate and poison the model's training dataset and sabotage the whole decision-making process. The attackers inject images of invalid users into multiple sets such that the model classifies them as valid users in the production. The paper also discusses a new mechanism which they call DEFEAT to protect the system against data poisoning. DEFEAT is a matrix that contains parameters derived from FaceNet (a deep neural network application, developed by Google).

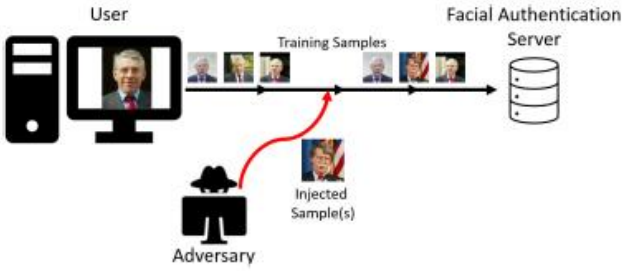

Fig 3: Proposed Data poisoning attack [15]

To derive the effectiveness of the data poisoning attack, the authors used two different datasets that is FEI: Facial Expression Images and LFW: Labeled Faces in the Wild. These data sets helped examine the attack in ideal and real-life backgrounds. The authors divided each data set into three parts to conduct this experiment: victims set, attacks set, and new user set. Each set has 15 photos per user, but in the victim set the authors replaced some of the actual user's photo with the attacker's photo from the attacker dataset. Now, the authors use 10 photos from each set to train the model and keep reaming 5 for testing once the model is trained. The paper mentions that with just 40% to 50% of poisoned training data, the attacker can achieve a success rate of 100% percent without any drop in the accuracy of the ML model which means that this data poisoning attack would go unnoticed.

To address this concerning finding the paper proposes the use of a DNN model which can act as a discriminator. The main feature of this discriminator would be to extract the features from the input facial image set and then analyze the distribution of features. With this simple implementation, 90 percent of data poisoning attacks can be detected. The authors also conducted comparison experiments with other proposed security mechanisms and DEFEAT was able to outperform all the other models even when very advanced techniques were used to poison the dataset to evade detection.

4.1.3 MEDIA EXTRACTION ATTACK

Safety mechanisms implemented to prevent the above two attacks have made sure that facial authentication is secure from a system design perspective, but one key aspect is yet not covered. What if the authentication system is fed a printed photo or video of the valid user? In the paper "EcoFace: Acoustic Sensor-Based Media Attack Detection for Face Authentication" [16] the authors have discussed in detail how content extracted from social media can be used to bypass the authentication system. The paper mentions that 53% of content that is downloaded just from Facebook and Google+ can be used to bypass any facial authentication system which is very concerning. The paper provides a detailed analysis of a proposed system using acoustic sensing including the hardware and software.

The main purpose of EcoFace is to differentiate between a live valid user and an attacker who is using any media content for forging the system. First, let us understand the construction of EcoFace, it is a plug-and-play system that uses the earpiece of the smartphone as a speaker to emit signals that are reflected to the system upon detecting the face. Now, the system collects those signals via two external microphones which were plugged in as part of EcoFace, and then these signals are processed to determine if it is coming off a live user or some media. The paper also explains how these signals are processed and analyzed but it is out of the scope of this survey. The efficiency of EcoFace is estimated to be 94.04% when experiments were conducted by varying the victim's photo or video presented flat or curved, the distance of media from the device, the background, and the time of the experiment. To make this method more efficient "Countermeasures to Photo Attacks in Face Recognition: A Public Database and a Baseline" [17] suggests maintaining a public database that would contain a repository of such signal analysis and different systems can refer to it to determine if they are under attack or if it is a valid user.

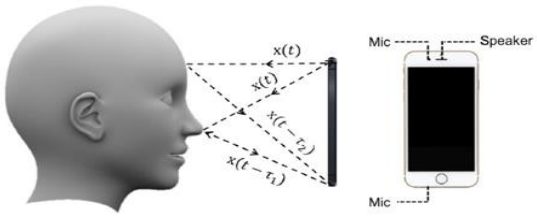

Fig 4: Working Principle of EcoFace [17]

4.1.4 PROPOSED SECURITY MECHANISM

The paper [18] proposes an enhanced authentication model for smart devices that can act as a defense mechanism against brute force attacks, eavesdropping, and even advanced attacks that use ML models to break into the authentication layer. The authors call this model a multi-modal authentication system that utilizes the face, periocular (eye socket), and iris for the authentication of any user. The paper talks about different subsystems that would be utilized for capturing, analyzing, recognizing, and then authenticating the user. On a high level here is how this new system would work, once a user is registered, the images of the user are then fed into the facial recognition system which uses an advanced ML-based model for learning about the features of the user. Then this subsystem passes the details to two other subsystems which use different techniques to store the information about the user and utilize it when the user tries to authenticate himself or herself. For experimenting with the proposed model, the authors choose 2 smart devices of Samsung i.e., Galaxy S5 and Galaxy Note 10.1

The authors have designed their proposed system with the following two components – 1) Feature Extraction Subsystems and 2) Comparison Subsystems. Each of these subsystems has various features underneath them and we will understand them one by one. Once a user is registered into the system its facial, periocular, and iris features are extracted using a Haar cascade-based detector which is a machine learning-based model that is deemed very advanced and secure. This model uses images from the training data set to map the most important and unique features of the current image. Once this classification is done it can be used by different features in the subsystem. Now here is how the system authenticates the user, the system works synchronously with the camera in the devices and provides feedback to the system. Once the camera detects the face of the user feature extraction subsystem comes into play. Scale Invariant Feature Transform (SIFT) extracts key features that are not dependent on the scale and orientation of the image. While SIFT is processing data Speeded-Up Robust Features (SURF) and Binarized Statistical Image Features (BSIF) come into play. SURF is very efficient in extracting information from images that are subject to change in scale and glare. Hence it is used for extracting key features of the periocular region of the face. With the help of filters, BSIF binarizes the image and extracts the feature of the iris from the image. Once all the key features are extracted from the images comparison subsystem uses Fast Approximate Nearest Neighbor Search (FANN) to compare and match the information extracted by SIFT and SURF and the Histogram matching technique is used to compare and match the iris information extracted by BSIF. After the successful match of all three features, a user is authenticated.

The paper provided a notion that this multimodal authentication system is more secure than long-existing and established authentication methods like PINs and patterns. The paper provides the results of the experiments they conducted using the proposed multi-modal authentication system on two devices. The results of these experiments show significant numbers like the Equal Error Rate (EER) was just 0.68% i.e., false acceptance and false rejection was just 0.68%.

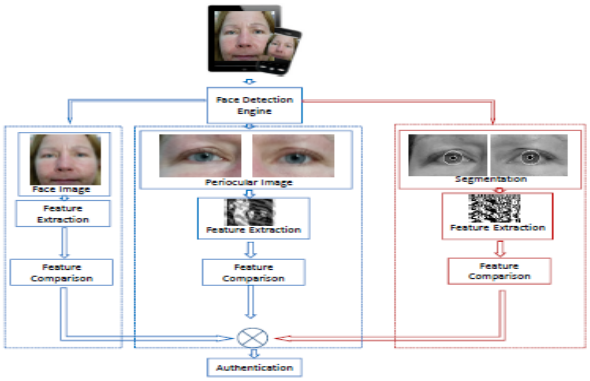

Fig 5: Proposed working of multi-modal System [18]

4.2 IRIS AUTHENTICATION

This section will focus on iris-based authentication. Iris refers to the part of your eye with color [8]. This can be used as a form of authentication by presenting your iris to a sensor to gain access to a system. Here we will look at how attackers can make use of this biometric.

4.2.1 PRINT ATTACK

The first attack on iris authentication we will look at is what is known as a print attack. A print attack is when an adversary presents a printed version of a biometric to a sensor to gain fraudulent access to a system. The writers of "On Iris Spoofing using Print Attack" conduct an experiment surrounding this attack. The goal of their study is to show how plausible it is for adversaries to successfully use a spoofed iris at a sensor [4]. This experiment is done using the IIS Database. This database contains hundreds of different irises with various versions of those irises. This means the database contained an iris with a transparent and colored contact lens version. On top of these versions, the researchers added their own printed versions of these irises to the database. This database allowed the researchers to present the collected irises at a sensor known as "VeriEye." This sensor will return a zero if it is an incorrect match and any number higher would be a genuine match. The researchers discovered that colored contact lenses would return a very low matching score and printed irises would return a rather high matching score. These results show us two things. The first is that adversaries can use colored contact lenses to avoid detection by iris sensors. The second is that it is very plausible for adversaries to gain access to a system using a printed image of a valid iris. This is a great study to reference when considering the goal of our paper because it explains how a simple attack can be successfully conducted. The last aspect of this paper to discuss is the proposed security implementations. The authors created an algorithm that applies image descriptors to these irises presented at the sensor. An image descriptor is data that defines specific factors of an image like the texture or color. This will allow them to apply specific variables to help the sensor detect false matches better. This is a very cost-effective way to deal with print attacks. What this tells us, among other mitigations we will look at, is that companies or entities that use biometric authentication overlook proposed simple solutions. This will be an important aspect to consider when making our conclusions.

4.2.2 SYNTHETIC GENERATION ATTACK

In the paper “Synthetic Iris Presentation Attack using IDCGAN” they showcase a form of presentation attack known as synthetic generation. Synthetic generation in this case means creating a fake iris using machine learning. They propose a new system known as the Deep Convolutional Generative Adversarial Network (iDCGAN) [3]. Like the last study, [4] the researchers here use a database of iris images. These images are used to allow their AI to learn iris patterns and output successful synthetically made irises. Through their results, it was determined that the AI had created high-quality images since it was trained to discard any others. Once the AI can create fake synthetic irises, the next step is to compare them to real irises. This step was conducted using a product we should know well, VeriEye. This product was used in both iris experiments we looked at because of its well-known commercial use. Like in the last study, VeriEye will give a zero for impostors and higher values for genuine matches. These tests led to results that show the synthetic irises have a false accept rate of about 67% [2]. Just like the last study we looked at, this shows that it is very plausible for adversaries to create fake iris images and fool a sensor. These results lead them to seek detection methods for synthetic irises. They use an algorithm known as DESIST. This algorithm is used to detect presentation attacks like synthetic generation and print attacks. However, DESIST was shown to not be able to successfully detect the synthetic images of iDCGAN compared to other synthetic generation AI. This is to show that our current standards for mitigation are not up to standard and could be easily thwarted.

4.3 FINGERPRINT AUTHENTICATION

A fingerprint is a pattern of ridges located on an individual’s finger [8]. Since these patterns are unique to an individual, we can authenticate ourselves based on this biometric. In this section, we will discuss attacks on this form of biometric authentication and its possible security issues.

4.3.1 SPOOFING ATTACK

Spoofing attacks on biometric authentication are a big point of concern. Throughout the discussion of spoofing, we will reference a couple of papers gathered through our survey techniques. First, we will define spoofing as it pertains to biometric authentication. Spoofing is an attack where an adversary steals a legitimate biometric to create a fake biometric that an authentication system will accept as a valid user [5]. This attack seems difficult to carry out but may not be as difficult as we initially thought. Spoofing attacks can be carried out on a variety of different biometrics like facial, fingerprint, and voice. This gives attackers a wide variety of paths and choices to carry out this attack. First, we will consider the attack being done using fingerprint data. An attacker must obtain the fingerprint data of a valid user before they can attempt to replicate their finger at a sensor. In the paper “Security Issues in Biometric Authentication,” they discuss a professor’s study/experiment on this type of attack [5]. The professor took two paths to conduct this study. First, the professor took fingerprint data from willing users. This allowed him to create a fake finger with their fingerprints to use at the authentication sensor. The results showed he was able to fool a wide variety of fingerprint readers rewarding him with about an 80% success rate. This high success rate is alarming, but it also requires that users are willing subjects. With that in mind, the likelihood of acquiring user fingerprints is low unless the bad actor is a savant at social engineering. Of course, you could also consider that the professor running this study could have been acquiring their biometrics under the guise of this experiment. The next method of acquiring the fingerprints is through surfaces the authenticated user has interacted with. This fingerprint would be enhanced with “super glue fumes” or an adhesive [5]. The fingerprint needs to be further enhanced by editing software. So, the adversary must get a digital picture of the fingerprint to edit. Then this image is transferred onto a “photosensitive printed circuit board” [5]. Once the mold was created of the fingerprint, the professor conducted his test. The results of this test were the same as the first test, there was an 80% success rate. Considering this is an actual way for an adversary to successfully collect fingerprint data, this success rate is worrying. We can conclude with this data that spoofing a fingerprint is very doable and successful for an attacker to do.

4.3.2 REPLAY ATTACK

Replay Attacks, often termed as type 2 attacks, occur within modules of biometric authentication software when previously intercepted biometric data is submitted to the sensor. The initiation of this attack involves intercepting biometric data through various means, such as capturing them using a scanner or compromising template databases. Following a thematic approach, we conducted a review of a case study titled "Replay Attack on Mobile Biometrics” [21].

This study outlines a continuous authentication framework in three phases for executing replay attacks. It involves capturing network and application logs each time a user interacts with the system. With remote access to legitimate logs, an attacker could generate or forge biometrics from the stolen information. These forged logs can be transmitted over a communication channel to a feature extraction module, generating a template based on multiple features and behavioral profiles. In the second phase, features necessary for estimating the effectiveness of replayed logs are determined. This is achieved by randomly selecting features and replacing a few legitimate features with attack features using a binary mask technique to simulate the scenario of an attack occurring randomly. This process is repeated for every attack, including a random log from another subject in the database to also assess zero-effort attacks using both feature representations.

The third phase involves comparing the Jaccard Matrix values for the input of legitimate features and combined features to the matching module. The value of the Jaccard Matrix is then compared with a threshold. If the value is greater than the threshold, a set of features would be dropped from the template, depending on the type of log it is. Thus, the template queue always consists of legitimate data. The accuracy of biometric systems is determined by the false positive rate, representing the proportion of replay attacks correctly passed as legitimate data. The likelihood of a successful replay attack increased from 2.3% to 40%, making it one of the most successful attacks in fooling a system. Biometrics are unique, and once stolen, cannot be recovered. Various security mechanisms are implemented to protect template data using approaches like folding transformation and perspiration of the biometric cryptosystem.

4.3.3 HILL CLIMBING ATTACK

An attack against the fingerprint system by submission of random templates in an iterative approach until the decision threshold crosses the matching score through an application [2]. It can be initiated by stolen templates, giving information about the image and template format. This experiment was performed on NFIS2 and MoC systems used for scanning and capturing fingerprint images. This experiment began by generating 100 synthetic templates of size 9x9 with fixed minutiae within each template designed by using the right and left fingerprint data of 75 users. Given as input, these templates are iteratively modified to design a template by adding, substituting, or deleting minutiae until a template is designed to achieve a high matching score. This is achieved by analyzing the patterns chosen corresponding to the iterations against the matching score. The threshold set for NFIS2 was 35 with 0.10FAR and 3.33FRR and 55 as a threshold for MoC with 0.16FAR and 17. 33FRR [2]. The efficiency of the Hill Climbing Attack is determined by the ratio of the mean number of iterations to the attempts of brute force attack. Post experiment, based on the success rate of the hill climbing attack for which the decision threshold was reached using fewer iterations than the brute force attack. We consider the NFIS2 system to be more robust against attack than the MoC system with a success rate of 40/150.

4.3.4 TEMPLATE DATABASE ATTACKS

The template is the digital representation of biometric data post-enhancement of the image. Template databases store encrypted transformation of biometrics and other information of the user used for the purpose of identification and verification during the authentication phase [19].

Template Reconstruction: An attacker being successful in modifying or reconstructing a new template for the existing ones by exploiting a database vulnerability, log data, information on cache, or cracking database accounts with administrative privileges would often form a base for replay or hill climbing attack by stealing or deleting the templates.

Circumvention: A result of a stolen template caused by a template attack to perform spoofing, replay attack, or administrative fraud by which an adversary can take control of the application to gain unauthorized access to sensitive data.

4.3.5 TEMPLATE PROTECTION SCHEMES

The proposed security method is to ensure user privacy by preventing guessing or reverse-engineering the key features of biometric data stored as templates. According to ISO/IEC 24745, it is said to be secure satisfying three factors non-invertibility, revocability, and unlikability [19]. It is the computational infeasibility of either generating original templates either from single or multiple protected biometric templates. A huge drop in the occurrence of breaches at the template module can be achieved by implementing security measures at the hardware, and software level and encryption of template information over the communication channel.

5. DISCUSSION

Following the evaluation of our three primary biometric authentication categories and associated research in these fields, our team started to analyze and discuss different aspects of biometric authentication in general. The focus of these discussions was to compare our findings to identify the potential scope of an attack and determine the future course of research/ attacks.

6.1 RESULT COMPARISON

It is pertinent to acknowledge that within the purview of this survey, all three categories of biometric authentication systems are susceptible to prevalent vulnerabilities, thereby exposing them to potential trivial attacks such as print attacks, spoofing attacks, and replay attacks. To fortify these systems against these common vulnerabilities and trivial attacks, various research papers propose distinct iterations of a particularly efficacious method—namely, liveliness detection. Our evaluation of findings from multiple papers yielded varying results, yet the collective evidence is sufficiently conclusive to assert that these common vulnerabilities can be mitigated with an accuracy exceeding 90 percent through the implementation of liveliness detectors, whether in the form of hardware or software. Each authentication system presents its unique challenges, prompting a diverse array of recommended security mechanisms tailored to address specific vulnerabilities. Amidst the rapidly evolving technological landscape, a prevailing theme in literature advocates the adoption of machine learning-based models as a proactive measure against attacks. However, as extensively deliberated, these very models are susceptible to attacks themselves, thereby posing a significant challenge and potentially rendering the overall system ineffective.

6.2 FUTURE RESEARCH/ATTACKS

In our discussion, we also included an agenda to discuss the potential areas for researchers to explore to make biometric authentication more dynamic and robust. One very interesting concept we discussed was the use of artificial intelligence to authenticate users by judging their responses to a current-day open question. This question can be from the current news, family background, courses taken, etc. This authentication system should be used as an additional layer of security to the biometric authentication system and ensure that this authentication system cannot be forged, replicated, or importantly forgotten. We also acknowledged the fact that the rapid growth of AI raises security threats for any authentication system and as part of this survey we decided to discuss very briefly potential security concerns for biometric authentication systems with the rise of AI. One risk we all agreed on was the use of AI to forge biometrics using 3D modeling, AI can used to create a very detailed 3D model of the human face, fingerprint, or any other form of biometric, and these detailed models can be 3D printed and used as fake biometric.

Furthermore, privacy emerged as a crucial consideration in our discussions. Given that biometric authentication involves storing sensitive data, the risk of data theft is a significant privacy concern. This potential vulnerability could lead to mass identity theft if biometric authentication is not secure enough. Conclusively, our research suggests that biometric authentication, while not deemed completely secure based on our survey of various papers, is

considered more robust than alternative authentication methods like PINs or passwords.

6.3 WORK DISTRIBUTION

We distribute our work across the semester to achieve maximum coverage of research papers. As discussed briefly in the survey technique section, every team member decided to spend at least 2 hours every week on individual research and 1-hour checkpoint call every Friday where we would collaborate/brainstorm and give status. Shivam Singh led the project and was responsible for finalizing the survey technique, initiating discussion points, facial authentication system, and maintaining the work distribution along with the project progress tracking. Michael Cooksey was responsible for defining the abstract and introduction, Iris authentication, spoofing of fingerprints, channeling all the discussions we had over this semester toward fruitful conclusions and proofreading all the documents before submission. Phaneendra Allu was responsible for the problem statement, related work, and fingerprint-based authentication system.

7. CONCLUSION

In conclusion, we see from all the presented evidence that biometric authentication security has its faults. In today's evolving world these faults will become gateways for adversaries. We have seen this from the various attacks presented and it is very plausible for attackers to conduct them. We have also seen the presented mitigations to ward off these attacks. Many cost-effective and well-made protocols are commonly overlooked. After reviewing all the provided evidence here, we can conclude that biometric authentication is not as secure as it can be. While this can be said of all aspects of cybersecurity, it is important to understand that biometrics are commonly overlooked when compared to other authentication means. This may tell us that the cybersecurity world is not ready for technological advancements that could allow attackers to launch more attacks on biometric authentication. Lastly, our call to action is for the enhancement of biometric authentication services to protect user's privacy and information.

REFERENCES

[1] Daksha Yadav, Naman Kohli, Shivangi Yadav, Mayank Vatsa, Richa Singh, and Afzel Noore. 2018. Iris presentation attack via textured contact lens in unconstrained environment. *2018 IEEE Winter Conference on Applications of Computer Vision (WACV)* (2018). DOI:http://dx.doi.org/10.1109/wacv.2018.00061

[2] Emma Lavens, Davy Preuveneers, and Wouter Joosen. 2023. Mitigating undesired interactions between liveness detection components in biometric authentication. *Proceedings of the 18th International Conference on Availability, Reliability and Security* (2023). DOI:http://dx.doi.org/10.1145/3600160.3604992

[3] Naman Kohli, Daksha Yadav, Mayank Vatsa, Richa Singh, and Afzel Noore. 2017. Synthetic Iris presentation attack using idcgan. *2017 IEEE International Joint Conference on Biometrics (IJCB)* (2017). DOI:http://dx.doi.org/10.1109/btas.2017.8272756

[4] Priyanshu Gupta, Shipra Behera, Mayank Vatsa, and Richa Singh. 2014. On Iris spoofing using print attack. *2014 22nd International Conference on Pattern Recognition* (2014). DOI:http://dx.doi.org/10.1109/icpr.2014.296

[5] Qinghan Xiao. Security issues in biometric authentication. *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.* DOI:http://dx.doi.org/10.1109/iaw.2005.1495927

[6] Rohit Agarwal and Anand Singh Jalal. 2021. Presentation attack detection system for fake Iris: A Review. *Multimedia Tools and Applications* 80, 10 (2021), 15193–15214. DOI:http://dx.doi.org/10.1007/s11042-020-10378-7

[7] Ruud M. Bolle, Jonathan H. Connell, and Nalini K. Ratha. 2002. Biometric perils and patches. *Pattern Recognition* 35, 12 (2002), 2727–2738. DOI:http://dx.doi.org/10.1016/s0031-3203(01)00247-3

[8] Sunil Swamilingappa Harakannanavar, Prashanth Chikkanayakanahalli Renukamurthy, and Kori Basava Raja. 2019. Comprehensive study of biometric authentication systems, challenges, and future trends. *International Journal of Advanced Networking and Applications* 10, 4 (2019), 3958–3968. DOI:http://dx.doi.org/10.35444/ijana.2019.10048

[9] Václav Matyáš and Zdeněk Říha. 2002. Biometric authentication — security and usability. *Advanced Communications and Multimedia Security* (2002), 227–239. DOI:http://dx.doi.org/10.1007/978-0-387-35612-9_17

[10] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. 2019.Security and accuracy of fingerprint-based biometrics: A Review. *Symmetry* 11, 2 (2019), 141. DOI: http://dx.doi.org/10.3390/sym11020141

[11] Lasher, B., Mulloor, J. and Russell, Z. (2022) Surveying Research on Biometric Authentication Methods in Computer-Simulated Reality [Preprint].

[12] Keshav, s. (2007) 'How to Read a Paper', Keshav [Preprint]. Doi: ACM SIGCOMM Computer Communication Review.

[13] Musa, A., Vishi, K. and Rexha, B. (2021) 'Attack analysis of face recognition authentication systems using fast gradient sign method', Applied Artificial Intelligence, 35(15), pp. 1346–1360. doi:10.1080/08839514.2021.1978149.

[14] Berghoff, C., Neu, M. and von Twickel, A. (2021) 'The interplay of AI and biometrics: Challenges and opportunities', Computer, 54(9), pp. 80–85. doi:10.1109/mc.2021.3084656.

[15] Cole, D., Newman, S. and Lin, D. (2022) 'A new facial authentication pitfall and remedy in web services', IEEE Transactions on Dependable and Secure Computing, 19(4), pp. 2635–2647. doi:10.1109/tdsc.2021.3067794.

[16] Chen, H. et al. (2020) 'Echoface: Acoustic sensor-based media attack detection for face authentication', IEEE Internet of Things Journal, 7(3), pp. 2152–2159. doi:10.1109/jiot.2019.2959203.

[17] Anjos, A. and Marcel, S. (2011) 'Counter-measures to photo attacks in face recognition: A public database and a baseline', 2011 International Joint Conference on Biometrics (IJCB) [Preprint]. doi:10.1109/ijcb.2011.6117503.

[18] Raja, K.B. et al. (2015) 'Multi-modal authentication system for smartphones using face, Iris and periocular', 2015 International Conference on Biometrics (ICB) [Preprint]. doi:10.1109/icb.2015.7139044.

[19] Security Vulnerabilities Against Fingerprint Biometric System Mahesh Joshi1 Bodhisatwa Mazumdar1 Somnath Dey1 {phd1701101004, bodhisatwa, somnathd}@iiti.ac.in 1 Indian Institute of Technology Indore, India

[20] Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-Garcia, JLA. Siguenza ATVS/Biometrics Research Lab, Escuela Politecnica Superior - Universidad Autonoma de Madrid C/ Francisco Tomas y Valiente, 1 1 - Campus de Cantoblanco - 28049 Madrid, Spain {julian.fierrez, femando.alonso, javier.ortega}@uam.es

[21] Tempestt Neal and Damon Woodard. 2019. Mobile biometrics, replay attacks, and behavior profiling: An empirical analysis of impostor detection. 2019 International Conference on Biometrics (ICB) (2019). DOI:http://dx.doi.org/10.1109/icb45273.2019.8987407

[22] Weaver, A. C. (2006). Biometric authentication. Computer, 39(2), 96-97

[23] Protecting Biometric-based Authentication Systems against Indirect AttacksHossein Malekinezhad, Hossein Ebrahimpour-Komleh Islamic Azad University Naragh Branch, University of Kashan

[24] Survey on Common Attack Vectors and Countermeasures of Fingerprint Systems ALI FATHI ALI SAWEHLI1 , NEIL ANDREW RUSSELL VIDOT 2 1,2 BSc (Hons) Cyber Security, Asia Pacific University, Kuala Lumpur, Malaysia

[25] Fingerprint Authentication and Security Risks in Smart Devices Muhammad Rehman Zafar Department of Computer Science Bahria University Islamabad, Pakistan Email: 01-243152-006@student.bahria.edu.pk Munam Ali Shah Department of Computer Science COMSATS Institute of Information Technology Islamabad, Pakistan Email: mshah@comsats.edu.pk

[26] K. Muthamil Sudar, P. Deepalakshmi, K. Ponmozhi, and P. Nagaraj. 2019. Analysis of security threats and countermeasures for various biometric techniques. 2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES) (2019). DOI: http://dx.doi.org/10.1109/incces47820.2019.9167745

[27] A. K. Jain, A. Ross and U. Uludag, "Biometric template security: Challenges and solutions," in 13th European Signal Processing Conference, 2005. IEEE, 2005, pp. 1–4

[28] Puja S Prasad. 2018. Vulnerabilities of biometric authentication systems: A survey. HELIX 8, 5 (2018), 4100–4103. DOI: http://dx.doi.org/10.29042/2018-4100-4103

[29] UNE, M., OTSUKA, A. and IMAI, H. (2008) 'Wolf attack probability: A theoretical security measure in biometric authentication systems', IEICE Transactions on Information and Systems, E91-D(5), pp. 1380–1389. doi:10.1093/ietisy/e91-d.5.1380

[30] Falmari, V.R. and Brindha, M. (2021) 'Privacy preserving biometric authentication using chaos on remote untrusted server', Measurement, 177, p. 109257. doi:10.1016/j.measurement.2021.109257